Alation Cloud Service

Alation User Documentation

Oct 23, 2024

TABLE OF CONTENTS

CHAPTER

ONE

STATUS PAGE

Alation Cloud Service

Important: The **Status Pages** apply only to Alation Cloud Service customers on the cloud-native architecture.

You can get real-time updates about Alation Cloud Service (ACS) by visiting the **Public Status Page** for ACS and the **Private Status Page** for your specific ACS instance(s). The status pages provide information about the health of ACS, incidents, and planned maintenance activities. You can also subscribe to updates to receive notifications about incidents and maintenance events.

The information provided on the status pages can help you identify incidents and plan further actions. You can always contact Alation Support for more help.

Alation provides two status pages:

- **Public Status Page**: This page shows the status of ACS by region for all shared services, incidents impacting multiple customers, and planned maintenance activities involving downtime. This page is open to any user. If there is an issue that impacts only an individual customer, the status will be reflected on the Private Status Page.
- **Private Status Page**: This page shows the status of customer-specific resources. Each customer has their own Private Status Page, and it's only visible to the specified Support Administrators for each customer.

1.1 Public Status Page

To access the Public Status Page:

1. Go to the Alation Help Center.
2. Click the **Alation Cloud Status** tile. The **Alation Cloud Status** landing page opens.
3. Click the **Public Status Page** tile.

You can also access the Public Status Page directly at https://status.alationcloud.com/.

1.1.1 Subscribe to Updates

You can subscribe to updates so you get notified about relevant events without having to visit the Public Status Page directly. You can subscribe to updates through:

- Email
- Slack
- Microsoft Teams
- SMS
- Atom/RSS feed
- Webhook

To subscribe to updates:

1. Click the **Subscribe to Updates** button in the upper right.
2. Select how you want to subscribe.
3. Follow the prompts and enter the relevant information. If asked to select a component or region, be sure to select only the region where your ACS instance is hosted.

Best Practice When Subscribing to Updates

Be sure to review carefully and only select the region that your ACS instance is hosted in. This will ensure that you only receive updates that are relevant to your ACS instance and do not receive updates regarding regions where you are not using Alation.

Anyone at your organization can subscribe to the Public Status Page. We recommend that anyone interested in planned maintenance events in particular subscribe to the Public Status Page.

1.1.2 View Overall System Status

The top center banner displays the most recent status across all services and will show a green bar that says **All Systems Operational** when everything is running smoothly.

1.1.3 View Component Status by Region

Below the main banner, you can see the current status of the shared production and development components of ACS:

- **Alation Cloud Service**: This shows the status of the ACS production environment.
- **Alation Cloud Service - Dev**: This shows the status of *ACS development environments*.

Each component can be expanded to view the status for each region.

1.1.4 View Maintenance Notifications

If there is a maintenance event, you will see a post on the Status Page under the **Scheduled Maintenance** heading. A maintenance notification includes:

- Title summarizing the maintenance activity
- Date of the maintenance
- Duration of the maintenance
- Status (Scheduled, In Progress, or Complete)
- Brief description of the maintenance actions being performed

If you are subscribed to updates, you will also receive a detailed notification about the maintenance.

Maintenance Stages

A planned maintenance event includes the following stages:

- **Scheduled Maintenance**: Each planned maintenance event that includes downtime starts with a scheduled maintenance post.
- **In-Progress Status**: When a planned maintenance has started, the maintenance event status is updated to **in progress**.
- **Completed Status**: When a planned maintenance is finished, the maintenance event status is updated to **completed**.

Maintenance Details

Click on the title of any Maintenance activity to view additional details. For activities that have not yet completed, there is also an option to subscribe to updates only for that specific incident. Alation recommends subscribing to the relevant components for your Alation Cloud Service deployments rather than specific incidents or activities only.

Maintenance History

Click **Incident History** at the bottom of the screen to see past events. To view the timeline of a planned maintenance activity, simply click on any activity in the history view to see the detailed timeline.

1.1.5 View Incident Notifications

If there is an active incident, you will see a post on the Status Page. The incident post includes the following information:

- The incident title describing the specific issue
- The incident status (Investigating, Identified, Monitoring, or Resolved)
- The time the message was posted
- Message about the incident
- Affected components

Note: If you are already subscribed to specific components or regions, you will automatically receive notices about specific incidents. You will not get notifications about incidents that only impact other components or regions.

1.1.6 View Incident Resolutions and History

Once an incident is resolved, it will be moved off the homepage and into the incident history. If you receive a notification about an incident and see no known issues when checking the Status Page, check the incident history to see if the incident has been resolved.

The incident history shows the details of each incident, including when it was identified and when it was resolved.

To view the incident history, click the **Incident History** link at the bottom of the page.

On the **Incident History** page, you can filter by component to help find a particular incident.

1.2 Private Status Page

To access the Private Status Page:

1. Go to the Alation Help Center.
2. Click the **Alation Cloud Status** tile. The **Alation Cloud Status** landing page opens.
3. Click the **Private Status Page** tile.

Important: The **Private Status Page** tile is only visible to the specified Support Administrator for each customer.

1.2.1 Subscribe to Updates

You can subscribe to updates so you get notified about events for your organization’s dedicated services without having to visit the Status Page directly. You can subscribe to updates through:

- Email
- SMS
- Webhook

To subscribe to updates:

1. Click the **Subscribe to Updates** button in the upper right.
2. Select how you want to subscribe.
3. Follow the prompts and enter the relevant information.

Best Practice When Subscribing to Updates

If your organization is running multiple instances of Alation Cloud Service, you can select which instances you would like to subscribe to for notifications. Alation recommends that support admins always subscribe to notifications about their production instance at a minimum. It is up to each individual whether they would like to also subscribe to notifications about any non production instances.

1.2.2 View Overall System Status

The top center banner displays the most recent status of your dedicated services and will show a green bar that says **All Systems Operational** when everything is running smoothly.

1.2.3 View Uptime

Below the main banner, you can see the uptime for your dedicated services for the past 90 days. Hover over a line on the graph to see a summary of the uptime status for that day.

If you have multiple instances, for example a production and development instance, click the plus sign to see the uptime for each instance separately.

Click the **View historical uptime** link to see a three-month calendar view of uptime status. Hover over a day to see the uptime status for that day. Click the dropdown to select which instance you want to view. You can also go back more than 90 days by adjusting the time period. At the top, you can click on the **Incidents** tab to see a list of past incidents.

1.2.4 View Incident Notifications

If there is an active incident, you will see a post on the Status Page. The incident post includes the following information:

- The incident title describing the specific issue
- The incident status (Investigating, Identified, Monitoring, or Resolved)
- The time the message was posted
- Message about the incident
- Affected components

1.2.5 View Past Incidents

On the homepage, click the **Incident History** link at the bottom of the page to see a list of past incidents. The incident history shows the details of each incident, including when it was identified and when it was resolved. Use the arrows to page through the list of resolved incidents. Click **Filter Components** to choose which instance you want to view.

CHAPTER

TWO

ACS OVERVIEW

Alation Cloud Service

Alation Cloud Service is a solution for organizations that wish to use the full scope of the Alation Data Catalog without the overhead associated with procuring and hosting the infrastructure for Alation instances, as well as configuring and maintaining the Alation application.

Alation Cloud Service is a fully managed instance cluster. The Alation experts prepare, install, and configure the required hardware and software. The Alation personnel takes the Alation application maintenance workload off the IT teams at an organization as all environment administration and upgrade tasks are delegated to Alation.

Cloud customers benefit from faster time to value as their instance is regularly patched and upgraded so that they can take advantage of new features, enhancements, and bug fixes shortly after they are released.

Important: To receive a demo of the Alation Cloud Services or request pricing options, contact your account manager. You can also sign up on the company site: Alation Cloud Service.

2.1 Geographic Availability

Alation Cloud Service

Alation Cloud Service is available in North America, Europe, and Asia Pacific.

If other locations are desired, you can raise this question with your account manager.

2.2 Cloud Networking

Alation Cloud Service

The following network options are supported:

- Whitelisting the Alation Cloud Service Internet Gateway on the corporate network (no additional cost)
- Enhanced networking with AWS PrivateLink (priced separately)

2.2.1 Whitelisting the Alation Cloud Service Internet Gateway

For those customers that support the whitelisting of the Alation Cloud Service NAT Gateway, Alation will send the NAT Gateway IP information. The IT team on the Customer side will need to whitelist the IP based on their network configuration.

For instructions, see *Whitelist the Alation Cloud Service IP*.

2.2.2 AWS PrivateLink

Alation Cloud Service supports the AWS PrivateLink option that provides private connectivity between VPCs, AWS services, and on-premises networks, without exposing your traffic to the public internet. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.

For Alation Cloud Service customers on the cloud-native architecture, support for PrivateLink was added in the 2023.1.5.1 release.

For instructions, see *AWS PrivateLink with Alation Cloud Service*.

2.3 Non-Production Environments in the Cloud

Alation Cloud Service

Available only for Alation Cloud Service customers on the cloud native architecture

Alation can provide non-production environments to Alation Cloud Service customers for testing, development, and training purposes. With a non-production environment, you can:

- Test out connecting to a new data source, from installing the connector to extracting metadata.
- Try out API calls without any risk to your production environment.
- Enable and try out previously unused features without any disruption to users in your main Alation instance.
- Train your users and let them try features in a safe way.

Non-production instances are available 52 weeks a year and are administered by Alation, just like your production Alation instance.

2.3.1 Non-Production Offerings

We offer two non-production plans:

- Cloud Developer Pro
- Cloud Developer Pro Plus

Features	Cloud Developer Pro	Cloud Developer Pro Plus
# of Objects	< 50,000	Same as your production instance
Refresh data from production to non-production	No	Yes
PrivateLink support	No	Yes

Cloud Developer Pro

Number of Objects

With Cloud Developer Pro, your non-production instance can have up to 50,000 objects.

Data Refresh

Data will not be synced with your production instance, so you'll have to manage the data on your Cloud Developer Pro instance separately.

PrivateLink Support

Cloud Developer Pro doesn't support connecting to data sources via AWS PrivateLink

Cloud Developer Pro Plus

Number of Objects

With Cloud Developer Pro Plus, your non-production instance can have as many objects as your production environment, so you can see exactly how changes you make will affect production.

Data Refresh

In addition, you can sync data from your production environment to non-production to ensure non-production is up to date. You can refresh your non-production instance up to once per quarter. To schedule a refresh, submit a request to Alation Support.

When you refresh your non-production data, all existing data and configuration in the non-production instance will be overwritten with whatever is currently in your production environment. All data and settings in your non-production instance should be identical to your production instance, with the following exceptions:

- Query schedules will be turned off
- Email notifications will be turned off
- Licensing for your non-production instance is handled separately

Everything else will be carried over, including users, identity provider configuration, connection settings, curated content, etc. If your production configurations are not applicable to your non-production instance, you'll need to make appropriate changes after the data is refreshed.

Note: When SAML or OIDC are set up, authentication on the non-production instance will use the same SAML or OIDC app that's used for production. See below for additional configuration steps to make sure authentication will work correctly on the non-production instance.

SAML and OIDC Configuration

SAML and OIDC configurations in Alation will be copied over to your non-production instance, but in order for authentication to work properly, you'll need to add the non-production instance URL to your identity provider.

SAML

For SAML, add the non-production instance sign-on URL in your identity provider's SAML application. The SAML application should include both the production and non-production sign-on URLs. In Okta, for example, you would add the URLs to the Other Requestable SSO URLs field.

OIDC

For OIDC, add the non-production instance's callback URL in your identity provider's OIDC application. The OIDC application should include both the production and non-production callback URLs. In Auth0, for example, you would add the URLs to the Allowed Callback URLs field.

PrivateLink Support

With Cloud Developer Pro Plus, you can connect to data sources via AWS PrivateLink.

2.3.2 Alation Agent with Non-Production Instances

An Alation Agent can only be associated with a single Alation instance at a time. If you use the Alation Agent, you'll need a separate Agent for your non-production instance. You'll have to install and configure the non-production Agent separately. You can use the non-production Agent to connect your non-production Alation instance to the same data sources as your production instance.

2.4 Cloud Service Security

Alation Cloud Service

Alation Cloud Service takes a robust approach to provide security for all our customers. To learn more, including information about specific security certifications, please reach out to your account manager.

By default, encryption keys are generated and rotated automatically for Alation Cloud Service deployments. You can also provide your own encryption keys using the Bring Your Own Key feature.

2.5 Alation Cloud Roles and Responsibilities

Alation Cloud Service

With Alation Cloud Service, all of the configurations or tasks on the backend of the Alation server will be performed by authorized Alation personnel.

Catalog users on the customer side with the Server Admin role can change the catalog settings and perform the configuration tasks available in the Alation UI.

Collaborative effort is required from both the Alation personnel and the customer admin team for a number of specific configuration tasks, such as setting up authentication or whitelisting the cloud instance IP on the corporate network.

See the table below for a breakdown of various activities and their respective owners:

Activity	Owner	Example
Application upgrade	Alation	• Upgrades to patch releases and major releases
Security	Alation	• Firewall configuration, pen testing, encryption
Backup management and backup restore	Alation	• Daily backups • Outdated backup cleanup • Backup restores
Disaster recovery setup and maintenance	Alation	• All disaster recovery setup and maintenance actions
Email server setup	Alation	• Setting up an email service
Backend admin tasks	Alation	• Enabling feature flags using **alation_conf** • Setting up Alation Analytics • Installing Alation Connector Manager
Server monitoring	Alation	• Monitoring the state of the Alation server and processes • Accessing server logs for troubleshooting

continues on next page

Table 1 – continued from previous page

Activity	Owner	Example
License deployment	Alation	• Managing application of licenses
Data migration	Alation and Customer	• Migrating an on-premise deployment to the Alation Cloud Service
SSO authentication setup	Alation and Customer	• Configuring SSO authentication for the Alation application and data sources. • SAML can be set up by the customer via the UI starting in 2021.4
Non-production environments	Alation and Customer	• Deploying and using a non-production cloud environment • Data refresh from production to non-production (customer requests it and Alation performs it).
AWS PrivateLink configuration	Alation and Customer	• Configuring AWS PrivateLink to connect to sources
IP whitelisting and FW access	Customer	• VPC, opening firewall ports, IP whitelisting
Data source setup	Customer	• Configuring data source connections in Alation UI
Alation Agent	Customer	• Installing the Agent • Upgrading the Agent • Maintaining and troubleshooting the Agent • Installing and managing data sources on the Agent

continues on next page

Table 1 – continued from previous page

Activity	Owner	Example
Administration in Alation UI	Customer	• Managing users and groups • Changing Catalog settings • Customizing Catalog page templates

2.6 Migrating from On-Prem to Cloud

Alation Cloud Service

It is possible to migrate from an on-prem deployment of Alation to the Cloud deployment. Alation Professional Services can assist in this move. Contact your account manager to start a conversation about moving to the Cloud.

CHAPTER

THREE

CONFIGURATION FOR THE CLOUD

Alation Cloud Service

Use this section for information about the Alation Cloud configuration tasks.

For information about providing your own encryption keys, see Bring Your Own Key.

3.1 Alation's IP Addresses for Allow Lists

Alation Cloud Service

Important: This page only applies if you're an Alation Cloud Service customer using our *cloud native architecture*, available from 2022.4.

This page contains a list of IP addresses that Alation Cloud Service's cloud native architecture uses to communicate with external resources, such as data sources, over the public internet.

Depending on your network security configuration, your IT or network administrator may need to add these IP addresses to an allow list so Alation can communicate with your network or data sources. You will need to allow the listed IP addresses for the geographic region that your Alation Cloud Service instance is in.

These IP addresses may change over time without notice. This document will be updated when IP addresses are changed or added.

3.1.1 IP Addresses

Geography	Location	CIDR	Range	Agent Connectivity Endpoint
Africa, Europe, & Middle East	Frankfurt	3.77.79.216/29	3.77.79.216 - 3.77.79.223	ocf.euc1.eu.alationcloud.com
	Dublin	3.253.238.240/29	3.253.238.240 - 3.253.238.247	ocf.euw1.eu.alationcloud.com
Americas	Montreal	15.156.224.56/29	15.156.224.56 - 15.156.224.63	ocf.cac1.ca.alationcloud.com
	Virginia	44.211.178.224/29	44.211.178.224 - 44.211.178.231	ocf.use1.alationcloud.com
	Oregon	18.246.160.64/29	18.246.160.64 - 18.246.160.71	ocf.usw2.alationcloud.com
Asia Pacific	Singapore	18.143.252.64/29	18.143.252.64 - 18.143.252.71	ocf.apse1.ap.alationcloud.com
	Sydney	3.27.127.216/29	3.27.127.216 - 3.27.127.223	ocf.apse2.ap.alationcloud.com
	Tokyo	52.195.197.8/29	52.195.197.8 - 52.195.197.15	ocf.apne1.ap.alationcloud.com

3.2 Whitelist the Alation Cloud Service IP

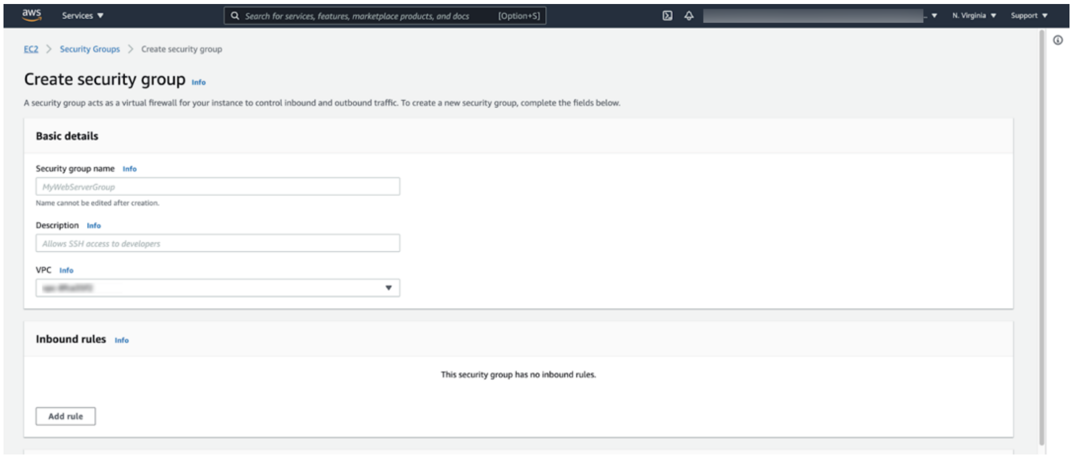
Alation Cloud Service

Use the steps in this section to whitelist the Alation Cloud Service IP on different network provider platforms where the instances are running under a public subnet and have a public IP.

3.2.1 Amazon Web Services

IPs are whitelisted in security groups under EC2 services.

1. In the EC2 service select the Security Group from the side panel:



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
[redacted]
N. Virginia ▼
Support ▼
EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

MyWebServerGroup

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

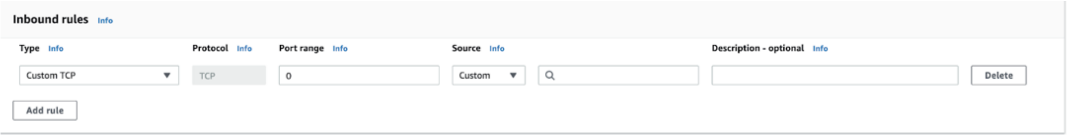
VPC Info

[redacted]

Inbound rules Info

This security group has no inbound rules.

2. Create a new security group and add the necessary protocol, port, and IP address CIDR:



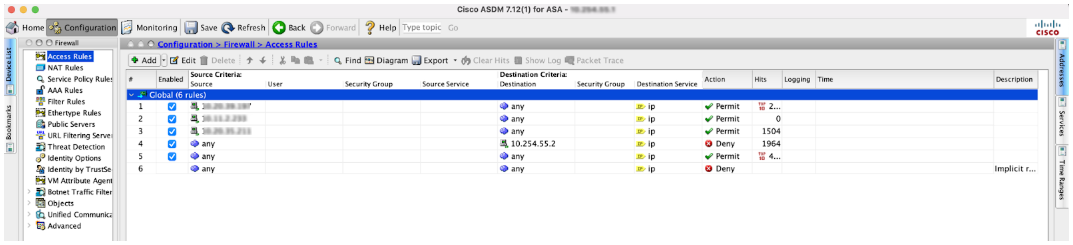
Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
Custom TCP ▾	TCP	0	Custom ▾	🔍		Delete

3. Attach the security group to the necessary instance to allow access.

3.2.2 Cisco

1. For accessing device configuration, log in with Cisco ASDM.
2. Access the **Access Rules**.
3. Add the new IP address and an action in order to whitelist the respective address:

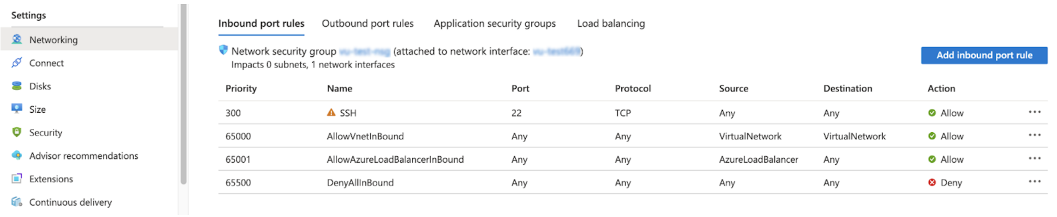


Cisco ASDM 7.12(1) for ASA - [redacted]

#	Enabled	Source Criteria:				Destination Criteria:			Action	Hits	Logging	Time	Description
		Source	User	Security Group	Source Service	Destination	Security Group	Destination Service					
Global (6 rules)													
1	☑	[redacted]				any		ip	✓ Permit	2...			
2	☑	[redacted]				any		ip	✓ Permit	0			
3	☑	[redacted]				any		ip	✓ Permit	1504			
4	☑	any				10.254.55.2		ip	✖ Deny	1964			
5	☑	any				any		ip	✓ Permit	4...			
6		any				any		ip	✖ Deny				Implicit r...

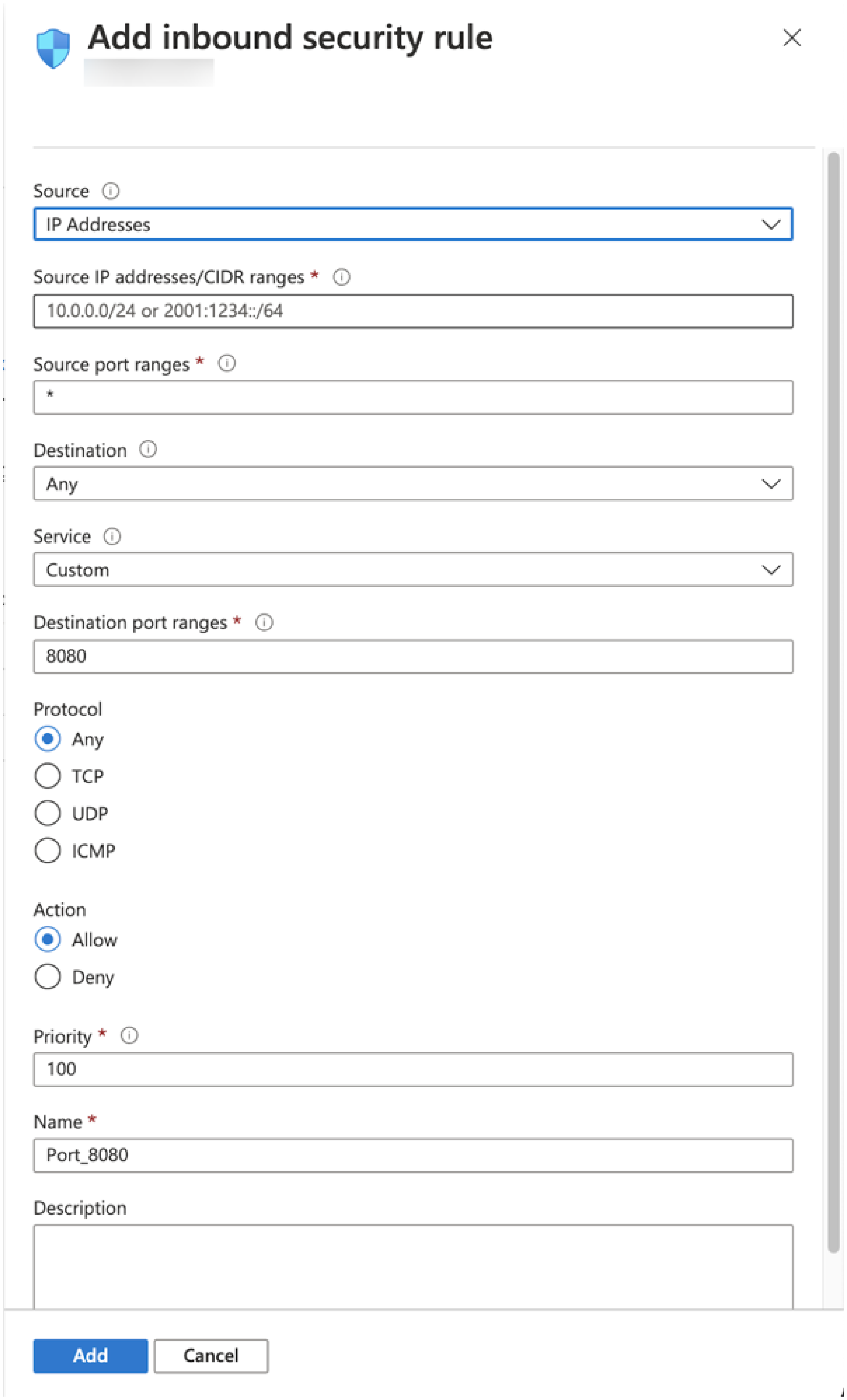
3.2.3 Azure

1. Login to the Azure console and navigate to **Virtual Machines**.
2. Select the VM.
3. Choose the network setting.
4. Add the corresponding inbound rules with the Source as IP Address and ports to whitelist:



Network security group [redacted] (attached to network interface: [redacted])
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action	
300	⚠ SSH	22	TCP	Any	Any	✓ Allow	···
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	···
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow	···
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny	···



Add inbound security rule

Source
IP Addresses

Source IP addresses/CIDR ranges *
10.0.0.0/24 or 2001:1234::/64

Source port ranges *
*

Destination
Any

Service
Custom

Destination port ranges *
8080

Protocol
● Any
○ TCP
○ UDP
○ ICMP

Action
● Allow
○ Deny

Priority *
100

Name *
Port_8080

Description

3.3 AWS PrivateLink with Alation Cloud Service

Alation Cloud Service

Amazon's AWS PrivateLink allows for secure connections between Alation Cloud Service and your AWS-based data sources.

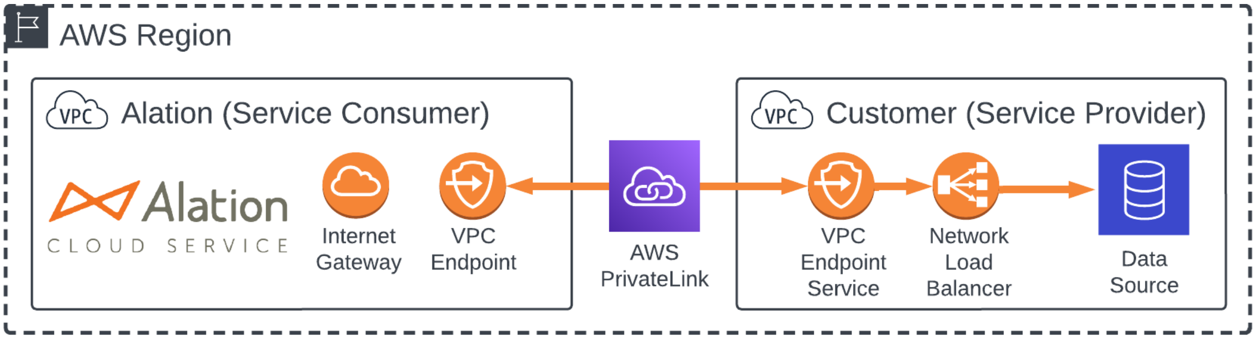
3.3.1 AWS PrivateLink Overview

AWS PrivateLink is a networking service that provides secure connectivity between AWS virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet.

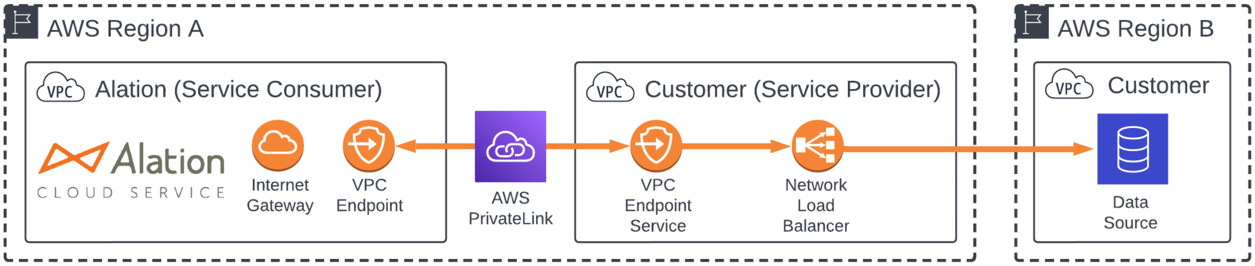
With PrivateLink, you can connect native AWS services and partner services, like Alation, to other AWS services, like your data sources that run in AWS. PrivateLink connections stay within AWS boundaries, so traffic through PrivateLink isn't exposed to the public internet. Data is only transmitted to Alation in response to requests from Alation Cloud Service.

Architecture

The following diagrams summarize the architecture of the PrivateLink networking option. Your VPC is the provider, and Alation's VPC is the consumer. See Amazon's PrivateLink documentation for more information about these concepts.



Your data source may be located in a different region, as long as you have a VPC in the Alation region that can serve as a transit connection for PrivateLink to your data source. The connection from the network load balancer to the data source is the responsibility of the customer.



Permissions

PrivateLink does not interact or interfere with Alation Identity and Access Management (IAM) settings or permissions. In terms of the seven-layer network model, PrivateLink operates primarily at the network layer, while Alation IAM settings and permissions operate at the application layer.

However, you must add permissions that allow specific AWS principals to create an interface VPC endpoint to connect to your endpoint service. This is documented below.

3.3.2 Set Up PrivateLink

Follow this procedure to create an AWS PrivateLink connection between Alation Cloud Service and a data source located in an AWS virtual private cloud (VPC).

The overall process involves three main steps:

1. *Create a Network Load Balancer in Your AWS Account*
2. *Create an Endpoint Service in Your AWS Account*
3. *Establish the Connection*

> **Warning:** This final step involves some back-and-forth between you and Alation Support. It also requires your Alation instance to be restarted, which will result in brief downtime. You'll be able to arrange an appropriate time for Alation Support to restart your instance.

Prerequisites

- Your data source must have network connectivity to an AWS virtual private cloud (VPC) that's in the same AWS region as your Alation Cloud Service instance.
- You need the IP address and port of the data source you're connecting to.

Create a Network Load Balancer in Your AWS Account

A network load balancer forwards incoming PrivateLink traffic to your data source. You can forward traffic to multiple data sources if needed. To create a network load balancer:

1. In the AWS Console, go to **EC2**.
2. Click **Load Balancers**.
3. Click **Create load balancer**.
4. Choose **Network Load Balancer**.
5. Click the **Create** button.
6. Fill out the **Basic configuration** section:
    a. For **Load balancer name**, enter a name that's unique within your AWS account.
    b. For **Scheme**, select **Internal**.
    c. For **IP address type**, select **IPv4**.
7. Fill out the **Network mapping** section:
    a. Select the **VPC** where your data source is located.

   b. Under **Mappings**, select the availability zones where your data source is located.

8. In the **Listeners and routing** section, choose the protocol and port for the connection coming into your load balancer.
9. If you have an existing target group with your data source in it, select it and proceed to the final step. Otherwise, click **Create target group**. A new tab will open. Fill out the following information:
   a. Select **IP addresses**.
   b. Enter a **Target group name**.
   c. Choose the protocol and port that's listening on your data source.
   d. Select the **VPC** where your data source is located.
   e. Click **Next**.
   f. Enter the IP address and port that's listening on your data source, then click **Include as pending** below.

   Note: If the IP address of your data source changes for any reason, you'll have to update your load balancer to route traffic from Alation to the new IP address.

   g. Click **Create target group**.
   h. Once the target is healthy, return to the load balancer tab.
10. Repeat the prior two steps for any additional data sources you may have.
11. Click **Create load balancer**.
12. For increased availability, scalability, and fault tolerance, we recommend turning on cross-zone load balancing:
   a. Click **View load balancer** to return to the list of your load balancers.
   b. Under **Load balancers**, click on the name of your load balancer to edit it.
   c. Click the **Attributes** tab.
   d. On the Attributes tab, click the **Edit** button.
   e. Enable the **Cross-zone load balancing** toggle.
   f. Click the **Save changes** button.

Once you've created a network load balancer, you need to create an endpoint service and associate it with the load balancer.

Create an Endpoint Service in Your AWS Account

1. In the AWS Console, go to **VPC**.
2. Click **Endpoint services**.
3. Click **Create endpoint service**.
4. Enter a name.
5. For **Load balancer type**, select **Network**.
6. Select the load balancer you created. If you just created it, it may take some time to become available.
7. Click **Create**.

8. Once the endpoint is created, take note of the **Service name**. You will need to provide the service name to Alation.

Now that you have an endpoint service connected to a network load balancer, you will work with Alation to establish the connection between Alation and your data source.

Establish the Connection

After creating the network load balancer and endpoint service, you will need to work with Alation Support to establish the connection between Alation and your data source.

1. Open a support ticket with Alation Support and provide the following information:
   a. **Subject:** AWS PrivateLink support requested
   b. **Body:**
      - Provide the endpoint service name.
      - Provide the port for connections coming into your load balancer (from *step 8* under Create a Network Load Balancer in Your AWS Account).
2. When Alation gets the support ticket, we'll send you an Amazon resource name (ARN) for the required IAM role.
3. Add the provided IAM role ARN as a principal to your endpoint service:
   a. Navigate to the endpoint service you created.
   b. Click the **Allow principals** tab, then the **Allow principals** button.
   c. Enter the **ARN** that Alation gave you.
   d. Click **Allow principals**.
4. Notify Alation that you've entered the IAM role ARN.
5. Alation will set up an endpoint in Alation Cloud Service, initiate the connection, restart your Alation instance, and notify you that it's ready. We'll also send the DNS name for the endpoint (you'll need it later for setting up your data source in Alation).

   > **Warning:** This step will require your Alation instance to be restarted, which will cause downtime. Arrange for an appropriate time with Alation Support.

6. Accept the incoming connection from Alation:
   a. Navigate to the endpoint service you created.
   b. Click the **Endpoint connections** tab. You should see a new endpoint listed.
   c. Select the endpoint.
   d. Click **Actions**.
   e. Click **Accept endpoint connection request**.
   f. In the confirmation that appears, type **accept** in the provided box, then click the **Accept** button. The VPC endpoint state will change to **Available**.

Your PrivateLink connection should now be active. Proceed to add your data source(s) to Alation as described below.

3.3.3 Add a PrivateLink-based Data Source in Alation

Once you've set up PrivateLink, the process for adding a PrivateLink data source in Alation is essentially the same as adding any other data source, with a few minor differences.

Host and Port

When adding your data source in Alation, the host name and port for the data source depends on your PrivateLink configuration.

- For the **host** name, use the DNS name that Alation provided when establishing the connection (see step 2 under Establish the Connection). This host name is unique to PrivateLink. If you don't know the host name, contact Alation Support.
- For the **port**, use the port for connections coming into your network load balancer (from *step 8* under Create a Network Load Balancer in Your AWS Account).

Note: For SQL Server data sources on PrivateLink, you may need to add `trustServerCertificate=true` to the connection string. This may be necessary if the SQL Server certificate has a domain name that's different from the VPC endpoint address.

Test the Connection

When you're done configuring your data source and endpoint service settings, test that the connection works. On the data source settings page, go to the **General Settings** tab and find the **Test Connection** or **Network Connection** section. Click the **Test** button.

If the test is successful, you can now use the data source for metadata extraction, query log ingestion, sampling, and profiling.

If the test fails, read the error message for information about what went wrong. Double check your connection information, such as the host name and port, and update it if needed. If you can't troubleshoot the error on your own, contact Alation Support.

Help with Adding Data Sources

For help with adding OCF data sources, see the /sources/OpenConnectorFramework/index section of the docs, then scroll down to find your specific data source.

For help adding native connectors, see /archive/DataSourceConfiguration/AddingaDataSource.

3.3.4 Add a New PrivateLink-based Data Source in AWS

If you've already set up a data source using PrivateLink in the past, you can add new data sources to your existing PrivateLink connection. A single PrivateLink connection can typically support up to 50 data sources, depending on your network configuration and traffic.

1. In the AWS Console, go to **EC2**.
2. Click **Load Balancers**.
3. Select the load balancer for your PrivateLink connection.
4. In the **Listeners** section, click **Add listener**.

5. If you have an existing target group with your data source in it, select it. Otherwise, click **Create target group**. A new tab will open. Fill out the following information:

   a. Select **IP addresses**.

   b. Enter a **Target group name**.

   c. Choose the protocol and port that's listening on your data source.

   d. Select the **VPC** where your data source is located.

   e. Click **Next**.

   f. Enter the IP address and port that's listening on your data source, then click **Include as pending** below.

   > **Note:** If the IP address of your data source changes for any reason, you'll have to update your load balancer to route traffic from Alation to the new IP address.

   g. Click **Create target group**.

   h. Once the target is healthy, return to the load balancer tab.

See **Add a Data Source in Alation** for remaining steps to set up your data source.

3.3.5 Migrate PrivateLink to Alation's Cloud Native Architecture

When you migrate to Alation's cloud native architecture, your Alation instance will move to a new VPC. You will need to make some configuration changes during the migration to ensure your PrivateLink data sources continue to work. These changes are described below.

> **Note:** The exact migration steps may vary. For example, the Alation engineer handling your migration may ask you to accept the new endpoint connection before migration instead of afterward. Work with your Alation account manager and Alation Support to determine the exact steps and schedule.

Endpoint Service Settings

Before migrating to Alation's cloud native architecture, you'll need to update your PrivateLink configuration to prepare for the migration. You'll need to accept a new incoming endpoint connection. In some cases, you may also need to add a new Amazon resource name (ARN) to your endpoint service.

To reconfigure PrivateLink before migrating to Alation's cloud native architecture:

1. If needed, Alation will provide you a new Amazon resource name (ARN) for the required IAM role. Add the provided IAM role ARN as a principal to your endpoint service:

   a. In the AWS Console, go to **VPC**.

   b. Click **Endpoint services**.

   c. Select the endpoint service you created.

   d. Click the **Allow principals** tab, then the **Allow principals** button.

   e. Enter the **ARN** that Alation gave you.

   f. Click **Allow principals**.

2. Notify Alation that you've entered the IAM role ARN.
3. Alation will initiate a new connection and migrate your Alation instance to the cloud native architecture. Your Alation instance will be offline during this process. We will notify you when it's back online.
4. Accept the incoming connection from Alation:

   a. Navigate to the endpoint service you created.

   b. Click the **Endpoint connections** tab. You should see a new endpoint listed.

   c. Select the endpoint.

   d. Click **Actions**.

   e. Click **Accept endpoint connection request**.

   f. In the confirmation that appears, type **accept** in the provided box, then click the **Accept** button. The VPC endpoint state will change to **Available**.

Data Source Settings

Once Alation has set up the new endpoint, we may send you a new DNS name for the data source. On the data source settings page in Alation, go to the **General Settings** tab and update the host name with the DNS name we provided.

If a private DNS name was previously created, it will remain the same, and you won't need to update your data source settings.

Test the Connection

When you're done configuring your data source and endpoint service settings, test that the connection works. On the data source settings page, go to the **General Settings** tab and find the **Test Connection** or **Network Connection** section. Click the **Test** button.

If the test is successful, you can now use the data source for metadata extraction, query log ingestion, sampling, and profiling.

If the test fails, read the error message for information about what went wrong. Double check your connection information, such as the host name and port, and update it if needed. If you can't troubleshoot the error on your own, contact Alation Support.

3.3.6 Limitations

Data Source Location

To use PrivateLink, your AWS-based data sources must have network connectivity to an AWS virtual private cloud (VPC) in the same AWS region as your Alation Cloud Service instance. To determine which AWS region your Alation Cloud Service instance is located in, contact your Alation account manager.

PrivateLink connections with data sources that are in cloud systems other than AWS, such as Azure, aren't supported by Alation at this time.

Number of Connections

You're limited to one PrivateLink connection per Alation Cloud Service instance. A single PrivateLink connection can typically support up to 50 data sources, depending on your network configuration and traffic.

3.4 Reconfigure Azure AD and Okta for Alation's Cloud Native Architecture

Alation Cloud Service

3.4.1 Background

Alation is introducing subdomains to the URL for Alation Cloud Service with the cloud native architecture. The change requires an admin of your Identity Provider to add the new URL to the identity provider, if you have previously configured the identity provider without the subdomain.

Region	Change	Example of New Domain
Europe	.eu subdomain	[customer-name].eu.alationcloud.com
APAC	.ap subdomain	[customer-name].ap.alationcloud.com
US	No change	Not applicable

3.4.2 Benefit

The new subdomains will provide the following additional benefits to Alation Cloud Service customers:

- **Regional identity:** It will be more clear to all end users that your data is hosted in your geography.
- **Performance and scalability:** Alation will be better able to optimize the performance of each region and to continue to scale the service.
- **Isolation and compliance:** The new subdomains will provide additional isolation between regions and improve compliance with local regulations.

3.4.3 Impact

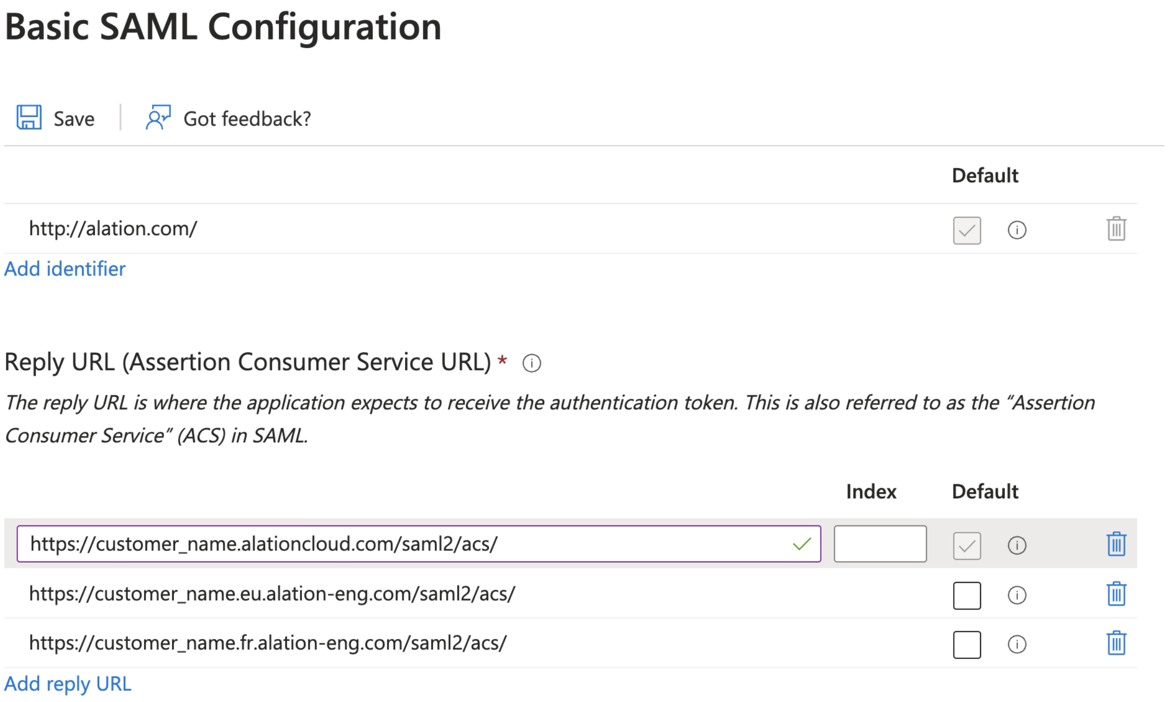
For the most common identity providers, Azure AD and Okta, the new URL can be added in such a way that the existing and new URL are both present.

Additionally, a redirect page will be in place to inform users visiting the old Alation URL that they are being redirected to the new URL.

3.4.4 Reconfigure Azure Active Directory (Azure AD)

To add the new Alation Cloud Service URL to Azure AD:

1. Go to the Azure AD SAML application.
2. Click on the single sign-on option.
3. Edit the **Basic SAML Configuration** option.



Basic SAML Configuration

	Default
http://alation.com/	☑

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://customer_name.alationcloud.com/saml2/acs/		☑
https://customer_name.eu.alation-eng.com/saml2/acs/		□
https://customer_name.fr.alation-eng.com/saml2/acs/		□

4. Add the new URL in the **Reply URL** section. Your new URL is the same as your old URL with either `.eu` or `.ap` before `.alationcloud.com`.

   Note: Default Checkbox

   Before migrating to the cloud native architecture, leave the **Default** checkmark on your old domain name.

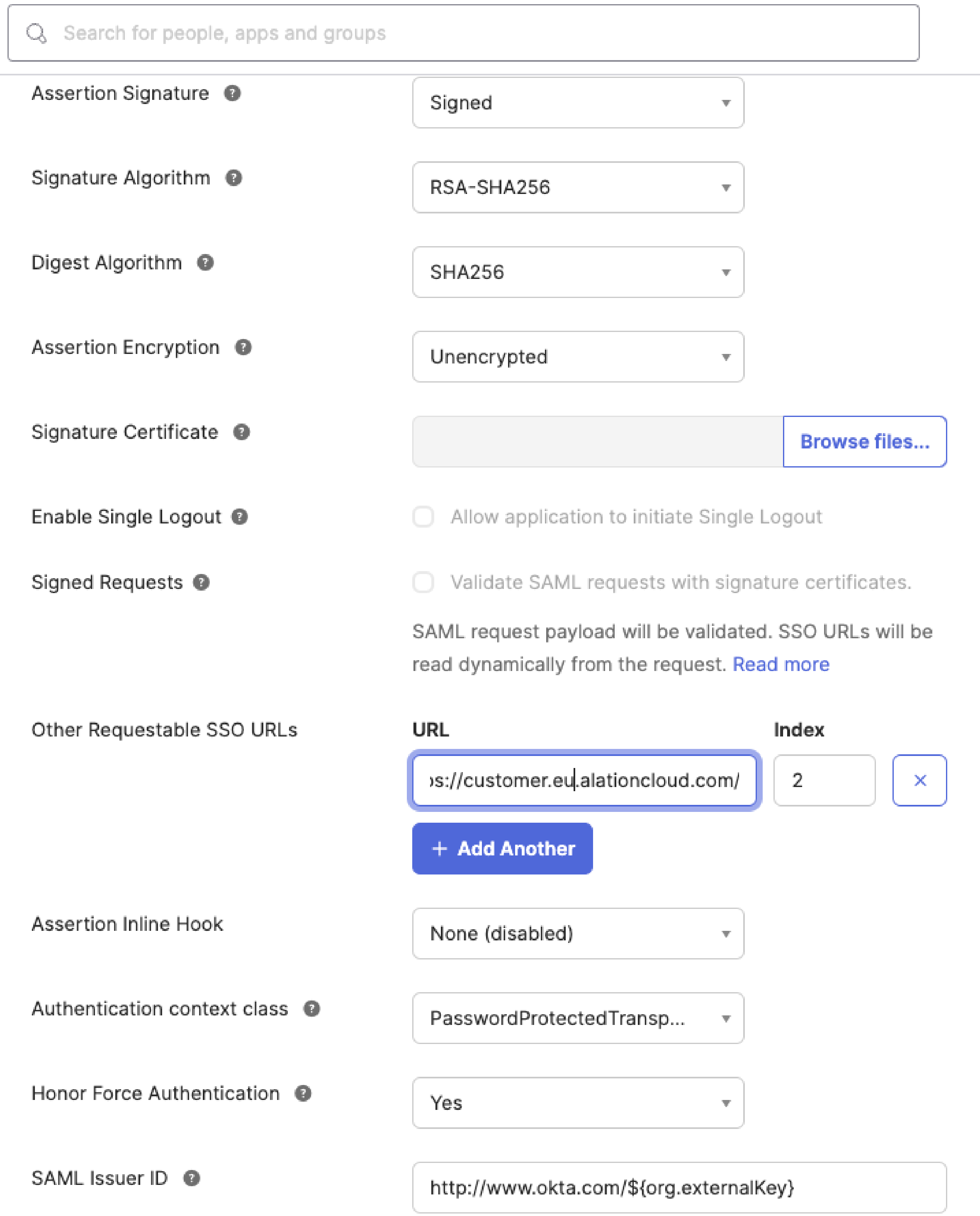
   After migrating to the cloud native architecture, we recommend changing the **Default** checkmark to the new domain name for performance benefits.

5. Click **Save**.

3.4.5 Reconfigure Okta

To add the new Alation Cloud Service URL to Okta:

1. Go to the Okta application.
2. Add new URLs in the **Other Requestable SSO URLs** section. Your new URL is the same as your old URL with either `.eu` or `.ap` before `.alationcloud.com`.



Search for people, apps and groups

Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Signature Certificate	Browse files...
Enable Single Logout	□ Allow application to initiate Single Logout
Signed Requests	□ Validate SAML requests with signature certificates. SAML request payload will be validated. SSO URLs will be read dynamically from the request. Read more
Other Requestable SSO URLs	URL: ›s://customer.eu.alationcloud.com/ Index: 2 + Add Another
Assertion Inline Hook	None (disabled)
Authentication context class	PasswordProtectedTransp...
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/${org.externalKey}

3.5 Cloud Service Configuration Limitations

Alation Cloud Service

3.5.1 Email Server Setup Limitation

Currently, the managed Cloud deployment of Alation does not support corporate email server setup. The built-in email server option has to be used until this functionality is added.

3.5.2 Alation Analytics V2 Limitations

Starting in 2023.3, Alation Cloud Service customers on the cloud native architecture can connect third-party BI tools to Alation Analytics V2.

If you are an Alation Cloud Service customer who's not yet on the cloud native architecture, contact your account manager to discuss your options.

3.5.3 Leaderboards

Leaderboards are by default turned off for Alation Cloud Service customers hosted in Europe. To have this feature turned on, create a Service Cloud ticket.

3.5.4 Custom Thumbnail Images on the Homepage

If a Server Admin wants to use custom images on the Alation Homepage, they can do so using an Article object in Alation. On how to add custom images using an Article object, see Use Custom Thumbnail Images.

You can also contact Alation Support to request the addition of new images to your Alation instance.

CHAPTER

FOUR

ALATION AGENT

Alation Cloud Service

The Alation Agent (or simply the Agent) is optional software you can install on your network to securely connect *Alation Cloud Service* to your on-premise data sources. After connecting the Agent to data sources that are behind your firewall, you can securely catalog metadata from those data sources to your Alation Cloud instance.

When considering use of the Agent, keep in mind the following:

- Each Alation Cloud Service instance can support multiple Agents in different geographical locations, network segments, or security zones.
- Each Agent can support multiple connectors and data sources.
- The Agent only works with connectors based on the Open Connector Framework (OCF). It doesn't support native or custom DB connectors.
- The Agent supports RDBMS, BI, and file system connectors.
- Newer versions of the Alation Agent now support Compose. See *Compose Compatibility* below for more details.

This page includes information about:

- *Agent System Requirements*
- *Architecture*
- *Security*

4.1 Agent System Requirements

Alation recommends running the Agent on a dedicated physical or virtual Linux machine with no other software installed. A virtual machine can be set up in a shared server environment as long as the required CPU, RAM, and HDD are allocated for the Agent.

You can install multiple Agents, each on its own machine, and connect them all with Alation Cloud Service. This may be needed if you have data sources in different geographical locations, network segments, or security zones.

4.1.1 Operating System

Alation Agent versions 1.5.0.2541 and later support the following operating systems:

- **Debian based:**
  - Debian 9, 10, and 11
  - Ubuntu 16, 18, 20, and 22
- **Red Hat based:**
  - AWS Linux 2
  - CentOS 7.x (x86 64-bit)
  - Fedora 33 and 34
  - Oracle Linux 7, 8, and 8.5 (on Red Hat Compatible Kernel)
  - Red Hat 7.x, 8.x, and 9.x (x86 64-bit)

Alation Agents *before* version 1.5.0.2541 support the following operating systems:

- **Debian based:**
  - Debian 9 and 10
  - Ubuntu 16, 18, and 20
- **Red Hat based:**
  - AWS Linux 2
  - CentOS 7.x (x86 64-bit)
  - Fedora 33 and 34
  - Oracle Linux 7, 8, and 8.5 (on Red Hat Compatible Kernel)
  - Red Hat 7.x and 8.x (x86 64-bit)

4.1.2 Hardware

The hardware requirements for the Agent depend on how many objects per data source you will be cataloging. Larger data sources require more hardware resources.

The Agent has been certified on the following hardware at the specified scale. For cases with more objects, connectors, or Agents, contact Alation.

		Small Deployment	Large Deployment
Scale	**# of objects per data source**	5 Million	15 million
	# of Agents per Alation instance	5	5
	# of connectors per Agent	5	10
System Component Requirements	**CPU**	2 or more cores 2.5-3.1 GHz	4 or more cores 2.5-3.1 GHz
	RAM	8 GB	16 GB
	HDD	20 GB	40 GB

The number of Agents per Alation instance may apply if you have data sources in different geographical locations, network segments, or security zones and need to install and connect multiple Agents to your Alation Cloud Service.

4.1.3 Alation Cloud Service Compatibility

In the table below, find the version of Alation you're currently using. To get the latest Alation Agent features and fixes, we recommend *upgrading* to the latest version of the Alation Agent that's compatible with your version of Alation Cloud Service.

Alation provides downloads for the latest two versions of the Alation Agent on the Customer Portal. Older versions of the Agent will become unavailable as newer versions are released.

Alation Agent Version	Compatible Versions of Alation Cloud Service
1.7.3.4537	2024.1.4, 2024.1.5, 2024.3
1.7.3.4452	2024.1.3, 2024.1.4, 2024.3

See the *Alation Agent Version History* page for a full listing of historical Agent releases and compatible Alation Cloud Service versions.

4.1.4 Checking the Agent Version

On the Agent host machine, check the installed Agent's version by running:

```
hydra version
```

The version number will be in the first line of the output.

4.1.5 Compose Compatibility

Compose Compatibility with the Agent

In order to use Compose with the Alation Agent, you must:

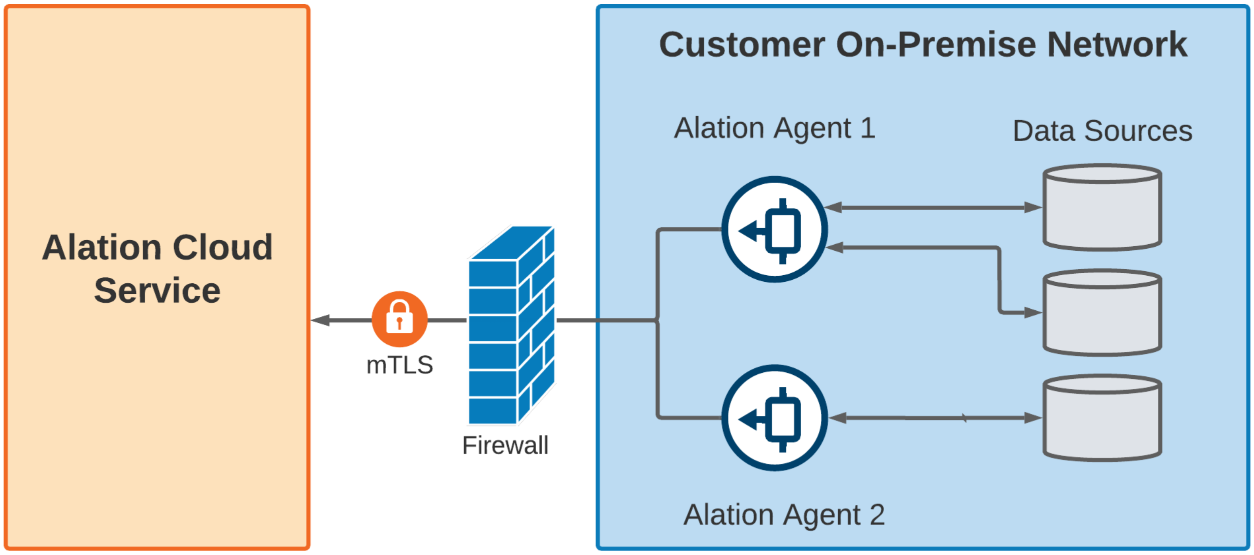
- Be on Alation Cloud Service version 2022.4 or later.
- Have Alation Agent version 1.2.1.868 or newer installed. Agent version 1.2.0.815 does not support Compose.
- Have a supporting version of the relevant connector installed on the Agent. See the documentation for individual OCF connectors to find out if a particular connector can connect to Compose through the Alation Agent.

4.2 Architecture

The Alation Agent is installed within your network and connects to the data sources as well as Alation Cloud Service. To connect to your data sources, the Agent uses connectors based on the Open Connector Framework (OCF).

Each Alation Cloud Service instance can support multiple Agents in different geographical locations, network segments, or security zones.

Each Agent can support multiple connectors and data sources.



4.3 Security

Alation designed the agent to comply with security policies that only allow outbound connections. It uses mutual TLS and end-to-end encryption to secure communications between the Agent and Alation Cloud Service.

4.3.1 Establishing a Secure Connection

Alation uses digital certificates to provide end-to-end encryption between the Agent and Alation Cloud Service. After installing the Agent software in your network, you'll generate a certificate signing request (CSR) on the Agent machine. You then upload the certificate signing request to the Alation Cloud Service. Alation Cloud uses the CSR to create a TLS certificate that is used to establish a trusted relationship between the Agent and Alation Cloud Service. You'll install this TLS certificate on the Agent to finalize the trusted connection.

Alation uses the AWS Certificate Manager (ACM) Private Certificate Authority for generating all Agent certificates. ACM is a highly-available private certificate authority service. Using ACM as the root certificate ensures that only certificates generated from that certificate authority can establish trusted communication with the Alation Cloud Service.

You can renew or revoke the certificate at any time. See *Work with the Agent's Certificates*.

Once the required certificate is in place, the Agent will initiate an outbound TLS v1.3 connection to Alation Cloud Service. The Agent and Alation Cloud Service will mutually authenticate.

- Alation Cloud Service validates that the Agent's certificate was signed by the ACM Private Certificate Authority.
- The Agent validates Alation Cloud Service's certificate authority trust chain, the certificate's expiration and revocation status, and the ID of your Alation Cloud instance.

4.3.2 Continuing Communication

This TLS connection ensures that all subsequent communication is fully encrypted and allows Alation Cloud Service and the Agent to transfer metadata during metadata extraction and query log ingestion. The connection is persistent, so future queries or extraction requests can be executed immediately.

If network interruptions ever break the connection between the Agent and your Alation Cloud instance, the Agent will attempt to reconnect. It keeps trying to connect using an exponential backoff algorithm. Once the Agent can connect to your Alation Cloud instance again, it will reauthenticate and reestablish a secure connection.

Any jobs, such as metadata extraction, that were underway will automatically restart as long as the connection is reestablished within 30 seconds. If it takes longer than that, you'll have to restart the job manually.

4.4 Further Reading

Explore the following topics for more help with the Alation Agent:

4.4.1 Agent Release Notes

Alation Cloud Service

See *Alation Cloud Service Compatibility* for information about which versions of Alation Cloud Service are supported by each version of the Agent. To get the latest Alation Agent features and fixes, we recommend *upgrading* to the latest version of the Alation Agent that's compatible with your version of Alation Cloud Service.

Release 1.7.3.4537

This patch release addresses a security vulnerability. (AL-166476)

Release 1.7.3.4452

The Alation Agent now creates the "alationdocker" Linux group (GID 41414). This group is used to access the Docker API socket from within the "agent" container running within Docker. This change was made in order ensure that external systems, such as SSSD, do not interfere with the operation of the Alation Agent by enforcing its own group IDs for well-known groups (such as the "docker" group). Users of the Alation Agent should take care to not delete, or otherwise modify, this group.

Release 1.7.2.4360

When the Alation Agent receives requests from Alation Cloud Service to connect to an on-premises data source, the Agent can now connect to AWS Secret Manager vaults within your Virtual Private Cloud (VPC) using an instance-based IAM role. This feature allows you to keep your data source credentials within your VPC so that they never traverse the Alation Cloud Service infrastructure. Moreover, these credentials will not be persisted in any Alation components, including the Alation Agent. For more information, see /sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/index.

To use this feature, you must meet the following requirements:

- You must be an Alation Cloud Service customer on the cloud-native architecture.
- You must be using *Alation Agent version 1.7.2.4360* or later. For help installing the Alation Agent, see *Install the Alation Agent*.
- To access AWS Secrets Manager using an IAM instance profile:
  - You must be on Alation Cloud Service version 2024.1.4 or later.
  - Your Alation Agent must be installed on an Amazon EC2 instance.
  - You must install *Authentication Service Add-on* version 5.14.0.1882 or later on the Alation Agent.
- To access AWS Secrets Manager using an IAM user's credentials:
  - You must be on Alation Cloud Service version 2024.1.5 or later.
  - You must install *Authentication Service Add-on* version 5.14.0.1968 or later on the Alation Agent.
- You must have a supporting OCF connector installed on the Agent. To find out if a specific connector supports this feature, see the documentation for the specific connector in the /sources/OpenConnectorFramework/index section.

> **Note:** You can use the Native Data Sources API to migrate a data source from an OCF connector that's not on an Alation Agent to an OCF connector that is on an Alation Agent.

(AL-149546)

Release 1.7.0.4045

- Notifications for Alation Agent's loss of connection and certificate expirations are now enabled by default for Server Admins. Existing preferences for Server Admins who have previously configured these notifications will remain unchanged. These notifications were previously opt-in by default. The change to opt-out by default aims to improve awareness and response to these important system events. Server Admins can adjust the notification settings under the **Notifications** tab on the **Account Settings** page. (AL-153656)
- The Agent diagnostic tooling for "ping" and TCP handshakes now support integrations with HTTP CONNECT proxies. (AL-151161)
- The test connection dialog for ETL data sources now indicates when the Agent is in polling mode. (AL-149017)
- Corrected an issue which would cause the connector application gateway to hang upon startup when operating for on-premise installations. (AL-154860)

Release 1.6.1.3465

Polling Mode UI

We've made some improvements in the Alation UI to help you understand when an Agent is in polling mode and how that could affect your connection:

- The Agent Dashboard indicates whether the Agent is in polling mode.
- When viewing connector details on the Connector Dashboard, you can see whether the connector is on an Agent that is in polling mode.
- When testing RDBMS data source connections on the data source settings page, you can see whether the data source is connected through an Agent that is in polling mode.

Release 1.6.1.3288

Polling Mode

The Alation Agent now supports connecting to Alation Cloud Service via polling mode.

Release 1.5.1.2863

Support for More Operating Systems

The Alation Agent now officially supports more operating systems:

- Debian 11
- Red Hat 9
- Ubuntu 22

For a complete list of supported operating systems, see the *Agent system requirements*.

Diagnostic Tool Improvements

The built-in *diagnostic tool* now checks that **/etc/hosts** is configured correctly. A missing or incorrect **/etc/hosts** file can disrupt the connection between Alation Cloud Services and the Alation Agent.

Release 1.5.0.2541

Diagnostic Tool

Is your Agent in a disconnected state? We've added a new diagnostic tool to the Agent that will help you troubleshoot connectivity issues. See the *Troubleshooting* topic for details on working with the diagnostic tool.

Release 1.3.0.1536

Bug Fixes

We fixed an issue where the Agent was failing to close old network connections when establishing failover connections to Alation Cloud Service.

Release 1.2.1.1168

Improved Reliability

The Alation Agent now establishes multiple failover connections to Alation Cloud Service for improved uptime and performance.

Support for Basic Authentication with Proxy

The Alation Agent now works with HTTP CONNECT proxies that require basic authentication. On the Agent machine, edit the **/etc/hydra/hydra.toml** file to include the following line:

```
web_proxy = "<username>:<password>@<proxy-address>:<proxy-port>"
```

Replace the parts in angle brackets with the appropriate information for your proxy.

See the *Agent installation instructions* for more details on configuring the Agent to work with a proxy.

Bug Fixes

We fixed an issue where the Agent could sometimes report an ERROR.E1000, which would prevent connectors from being installed. Upgrading to version 1.2.1.1168 resolves this issue.

Release 1.2.1.1120

Compose Support

The Alation Agent now supports Compose connections to on-premise data sources. This support includes:

- Query execution in Compose
- Query forms
- Scheduled queries
- Excel live reports
- Data upload

Compose Compatibility with the Agent

In order to use Compose with the Alation Agent, you must:

- Be on Alation Cloud Service version 2022.4 or later.
- Have Alation Agent version 1.2.1.868 or newer installed. Agent version 1.2.0.815 does not support Compose.

- Have a supporting version of the relevant connector installed on the Agent. See the documentation for individual OCF connectors to find out if a particular connector can connect to Compose through the Alation Agent.

Release 1.2.1.868

Multiple Agent Installations

Alation now supports multiple Alation Agent installations per cloud instance. Multiple Agents may be required if data sources are in different geographical locations, network segments, or security zones. A Server Admin for a cloud instance can now install Alation Agent multiple times to enable connection to on-premise data sources from the catalog.

Agent Enhancements

- Users can now delete an Agent even when the certificate is revoked.
- The default port of **80** for `web_proxy` is now honored by the Agent. Previously port **80** was incorrectly ignored and defaulted to **3128**.

4.4.2 Install the Alation Agent

Alation Cloud Service

Installing the Alation Agent (Agent) involves the following steps:

- *Step 1: Prepare for the Installation*
- *Step 2: Download and Run Installation Script*
- *Step 3: Name Your Agent*
- *Step 4: Generate Encryption Certificates*
- *Step 5: Install the Authentication Service Add-on (Optional)*

These steps are described in detail below. You will be switching back and forth between Alation and the Agent's host machine to complete the installation. You'll use information provided in Alation to run commands on the Agent machine, and you'll sometimes copy the output of those commands back into Alation.

You can install multiple Agents, each on its own machine, and connect them all with Alation Cloud Service. This may be needed if you have data sources in different geographical locations, network segments, or security zones.

Step 1: Prepare for the Installation

Before you can install the Agent, you must:

1. Make sure you have the Server Admin role in Alation.
2. Provision a Linux host to install the Agent on.
   - Check the *System Requirements* for the required hardware and software.
   - The Agent's host can be a physical or virtual machine. A virtual machine can be set up in a shared server environment, as long as the system requirements are met.
   - The Agent machine should be located appropriately within your network so that it can access the relevant data sources.
   - Don't run other software on the Agent machine—only the Agent should be installed.
3. Ensure that outbound port 443 is open.
4. Check that the Agent host machine can resolve the Agent connectivity endpoint for your region from the table below.

Geography	Location	Agent Connectivity Endpoint
Africa, Europe, & Middle East	Frankfurt	ocf.euc1.eu.alationcloud.com
	Dublin	ocf.euw1.eu.alationcloud.com
Americas	Montreal	ocf.cac1.ca.alationcloud.com
	Virginia	ocf.use1.alationcloud.com
	Oregon	ocf.usw2.alationcloud.com
Asia Pacific	Singapore	ocf.apse1.ap.alationcloud.com
	Sydney	ocf.apse2.ap.alationcloud.com
	Tokyo	ocf.apne1.ap.alationcloud.com

   You will need to make sure you have SSH credentials to the Agent machine and that it has outbound access to the open internet. If you do not want the Agent to have outbound access to the open internet, you may use a proxy server. In that case you will need to whitelist the Agent connectivity endpoint on your proxy server to allow the Agent machine outbound access to Alation Cloud Service.

   Note: If your proxy server is a TLS middlebox, additional steps are required. Contact Alation Support for more information.

   Then you can use a tool such as **dig** or **nslookup** to see if you can reach your Agent connectivity endpoint. For example:

```
dig <your-agent-connectivity-endpoint>
```

   If your Agent connectivity endpoint is reachable, the output of the **dig** command should include something like this:

```
;; ANSWER SECTION:
<your-agent-connectivity-endpoint>. 60 IN A <alation-cloud-IP>
```

   If your Agent connectivity endpoint is not reachable, you will need to configure your network to correctly resolve it.

5. Make sure you have access to the Customer Portal so you can download the Agent and connector installation packages. If you don't have access, contact Alation Support.

6. Optionally, contact Alation Support to request the Authentication Service add-on. The Authentication Service add-on enables the Agent to integrate directly with AWS Secrets Manager, so your data source credentials never leave your network. For information about how this integration works, see /sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/index.

   To use this feature, you must meet the following requirements:

   - You must be an Alation Cloud Service customer on the cloud-native architecture.
   - You must be using *Alation Agent version 1.7.2.4360* or later. For help installing the Alation Agent, see *Install the Alation Agent*.
   - To access AWS Secrets Manager using an IAM instance profile:
     - You must be on Alation Cloud Service version 2024.1.4 or later.
     - Your Alation Agent must be installed on an Amazon EC2 instance.
     - You must install *Authentication Service Add-on* version 5.14.0.1882 or later on the Alation Agent.
   - To access AWS Secrets Manager using an IAM user's credentials:
     - You must be on Alation Cloud Service version 2024.1.5 or later.
     - You must install *Authentication Service Add-on* version 5.14.0.1968 or later on the Alation Agent.
   - You must have a supporting OCF connector installed on the Agent. To find out if a specific connector supports this feature, see the documentation for the specific connector in the /sources/OpenConnectorFramework/index section.

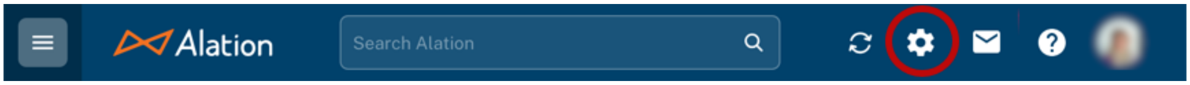
   Note: You can use the Native Data Sources API to migrate a data source from an OCF connector that's not on an Alation Agent to an OCF connector that is on an Alation Agent.

Step 2: Download and Run Installation Script

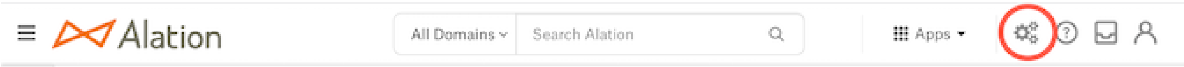
You're now ready to download the software package and run the installation script. You must have the Server Admin role in Alation to complete the remaining steps.

1. Click on the **Settings** icon in the top right corner.

   New User Experience



   Classic User Experience



2. **New User Experience**

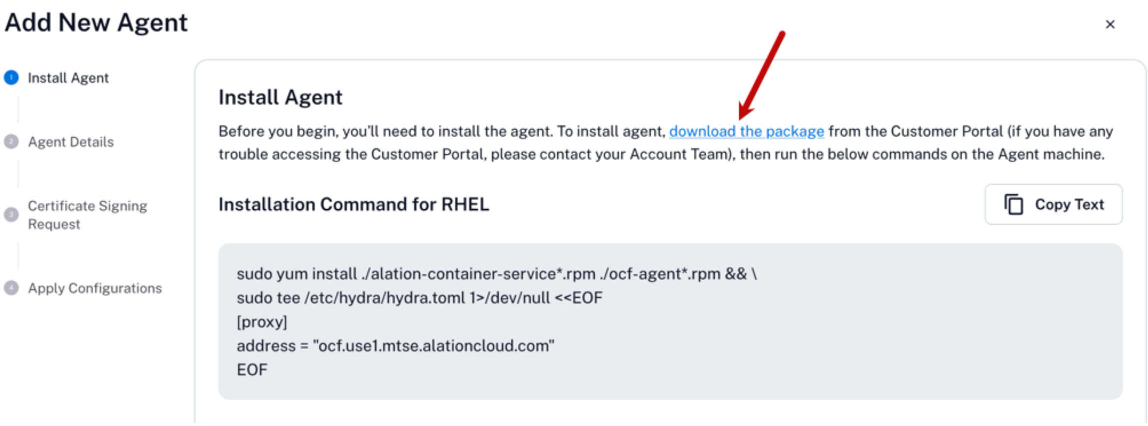
   The **Admin Settings** page appears. Under the **Platform Settings** section, click **Agents**.

   Classic User Experience

   Under the **Server Admin** section, click **Manage Connectors**. Then click the **Agents** tab. The **Agents Dashboard** appears.

3. Click the **Add New Agent** button. The **Add New Agent** dialog will appear.
4. In the **Add New Agent** dialog, click the **download the package** link to open the Alation Customer Portal.

   New User Experience



Add New Agent

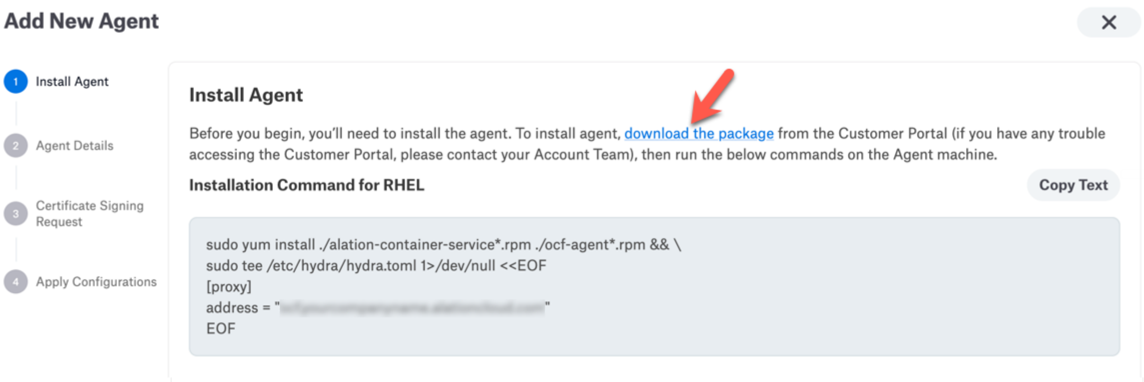
Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "ocf.use1.mtse.alationcloud.com"
EOF
```

   Classic User Experience



Add New Agent

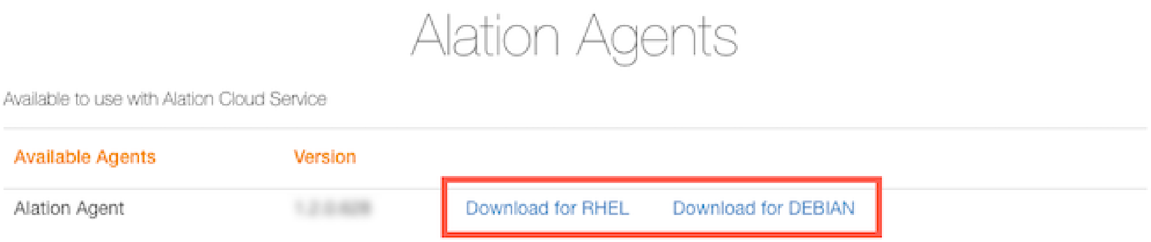
Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

5. In the Alation Customer Portal, select the latest available version for the desired operating system:
   - **RHEL** for Red Hat-based systems
   - **DEBIAN** for Debian-based systems



Alation Agents

Available to use with Alation Cloud Service

Available Agents	Version		
Alation Agent	[redacted]	Download for RHEL	Download for DEBIAN

   The Agent will download to your computer as a tar.gz file named **ocf-agent-<agent-version>-<operating-system>.tar.gz**.

6. If needed, transfer the downloaded file to the Agent's host machine. For example, if you downloaded the Agent file to a Unix-based machine, you could transfer the file using the scp command in Terminal:

```
scp /local/path/to/ocf-agent-<agent-version>-<operating-system>.tar.gz <ssh-user>@
<server-address>:/remote/path/to/ocf-agent
```

7. On the Agent's host machine, extract the **.tar.gz** file. Example:

```
tar -xf ocf-agent-<agent-version>-<operating-system>.tar.gz
```

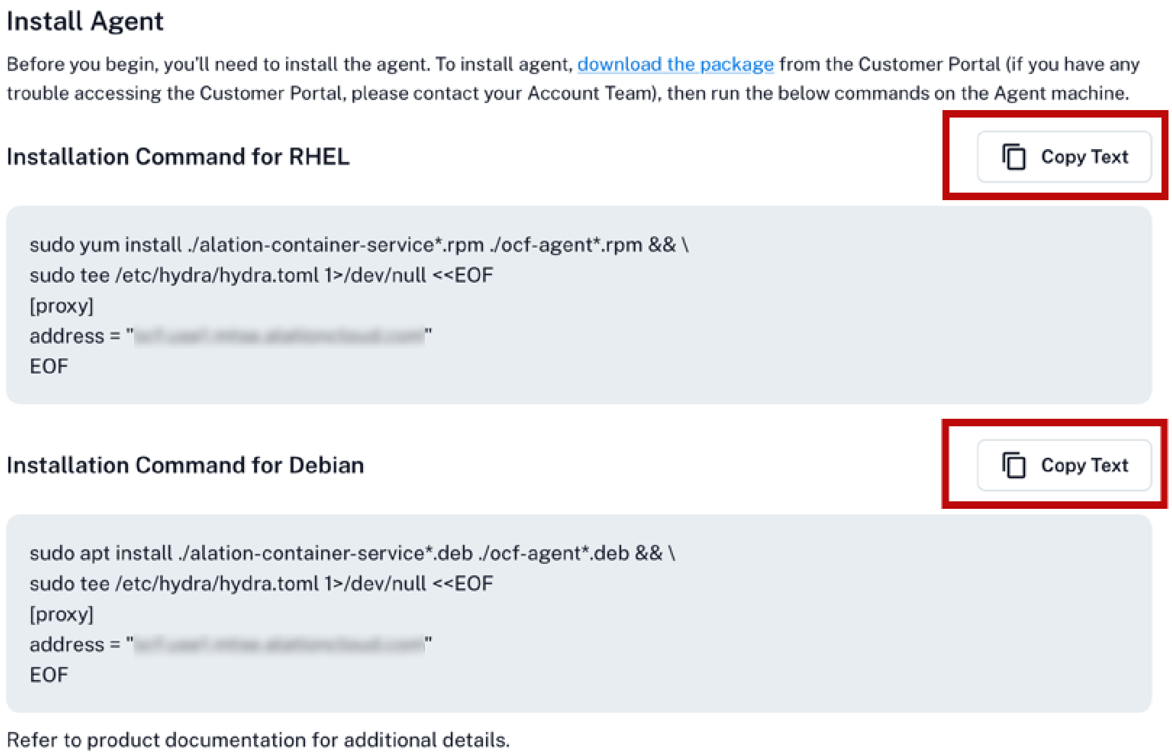
   The Agent installation files are extracted into an **ocf-agent** directory.

8. Change into the ocf-agent directory.

```
cd ocf-agent
```

9. In Alation, copy the relevant installation command from the **Install Agent** screen.

New User Experience



Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

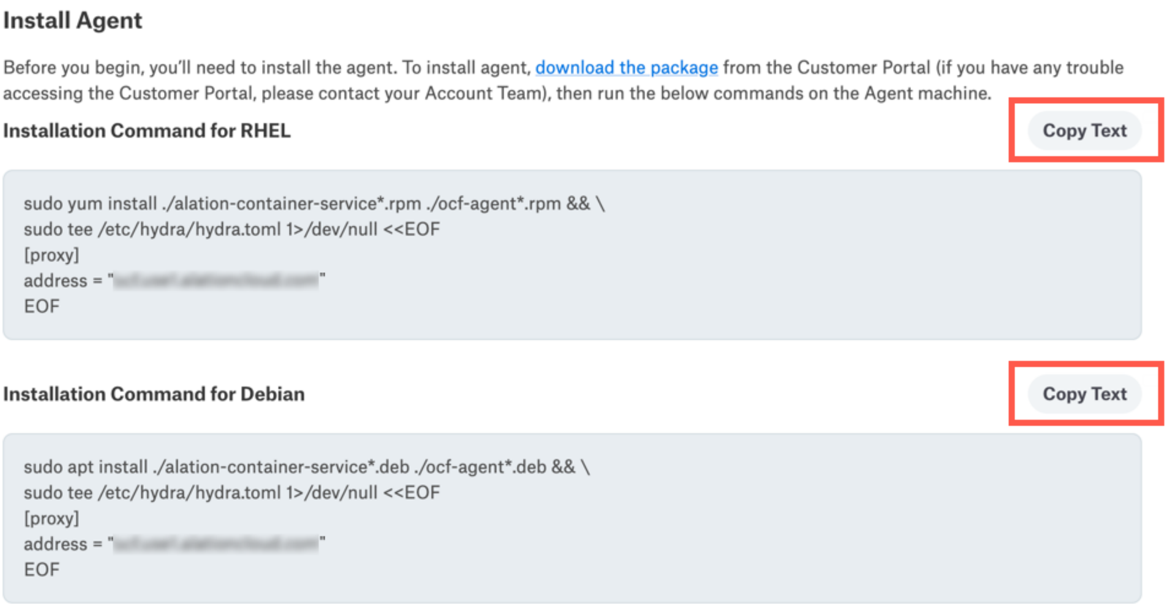
```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Installation Command for Debian

```
sudo apt install ./alation-container-service*.deb ./ocf-agent*.deb && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Refer to product documentation for additional details.

Classic User Experience



Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Installation Command for Debian

```
sudo apt install ./alation-container-service*.deb ./ocf-agent*.deb && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

10. In the terminal on the Agent's host machine, make sure you are in the **ocf-agent** directory, then paste and run the installation command. This will install and configure the Agent.
11. *(Optional)* If your network routes outgoing traffic through an HTTP CONNECT proxy, see the Advanced Configuration section below.
12. In Alation, click the **Next** button.

You have now installed and configured the Agent on a machine inside your network. Next you'll need to name the Agent in Alation.

Advanced Configuration

If your network routes outgoing traffic through an HTTP CONNECT proxy, you need to:

- Add the Alation Cloud Service connectivity endpoint to your proxy server's allow list.
- Add the proxy's address to the Agent configuration file.

Proxy Allow List

You will need to add the Alation Cloud Service connectivity endpoint to your proxy server's allow list so the Agent can reach your Alation Cloud Service instance.

The Alation Cloud Service endpoint is shown on the `address` line of the Agent installation command. This is the same address that should be in your Agent configuration file at **/etc/hydra/hydra.toml**.

Add Proxy Address to Agent Config

This is done on the Agent's host machine. The steps depend on whether your proxy requires authentication.

- **No Authentication**

  For proxies that don't require authentication, edit **/etc/hydra/hydra.toml** to add the following line:

```
web_proxy = "<proxy-address>:<proxy-port>"
```

- **Basic Authentication**

  Starting with Agent version 1.2.1.1168, you can route the Agent through proxies that require basic authentication. Edit **/etc/hydra/hydra.toml** to add the following line:

  ```
  web_proxy = "<username>:<password>@<proxy-address>:<proxy-port>"
  ```

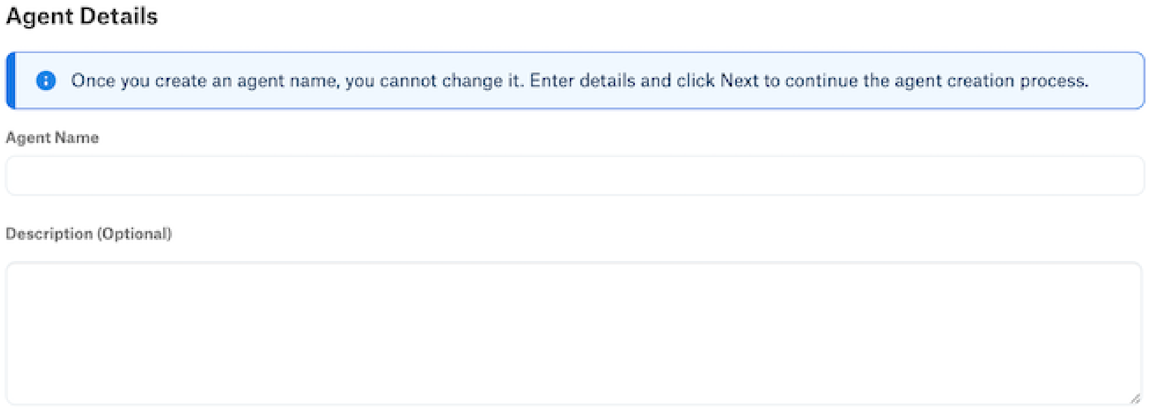
  Replace the parts in angle brackets with the appropriate information for your proxy. Don't include the angle brackets. Do include the quotes. The proxy address can be a domain name or an IP address. If no port is provided, the Agent defaults to port 80.

  Here's an example with basic authentication:

  ```
  web_proxy = "jane:securepassword@company.proxy.com:3128"
  ```

Step 3: Name Your Agent

1. In Alation, enter a name for the Agent. This name can't be changed, so choose carefully.

   Agent Details

   Once you create an agent name, you cannot change it. Enter details and click Next to continue the agent creation process.

   Agent Name

   Description (Optional)

   Note: The Agent's name is used to identify connectors that you install on this Agent. When you install a new connector or add a new data source and link it to your Agent, you'll see the Agent name added to the end of the connector name.

2. *(Optional)* Enter a description of the Agent. This appears on the Agent's detail page. The description can't be changed later.

3. Click the **Next** button, then confirm the name you chose.

Now that you've named the Agent, it's time to establish the secure connection between your Alation Cloud Service instance and the Agent.

Note: After starting the Add Agent workflow you can always close the Add New Agent dialog. You can pick it back up again at a later time by returning to the Agent Dashboard and clicking on the **Complete Setup** link.

Step 4: Generate Encryption Certificates

Alation uses signed certificates to encrypt the communication between Alation and the Agent.

1. On the **Generate Certificate Signing Request (CSR)** screen, copy the provided command and run it on the Agent's host machine.

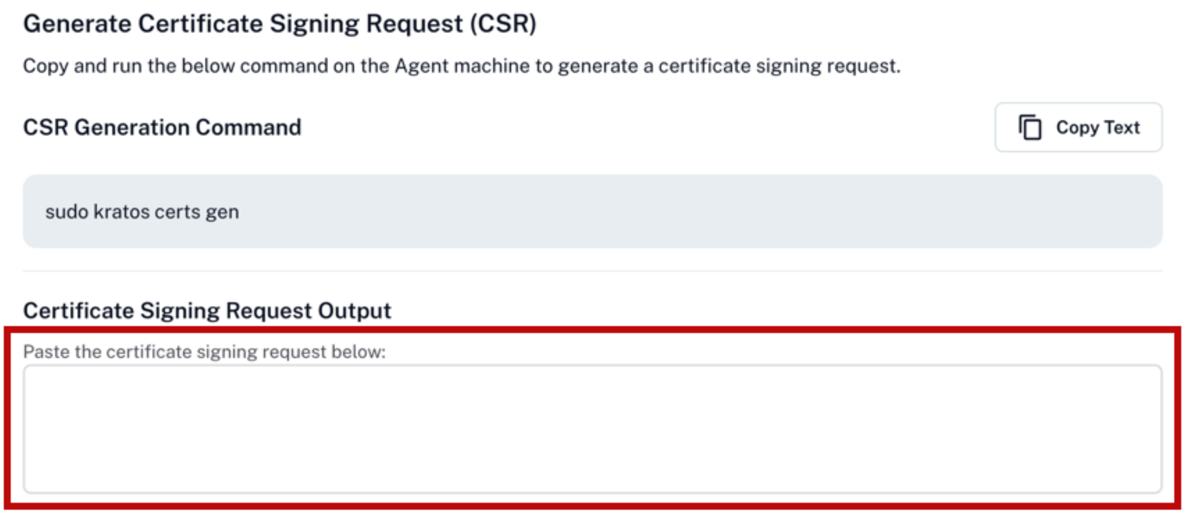
   ```
   sudo kratos certs gen
   ```

   The command will generate a certificate signing request. Example output:

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   <your certificate signing request>
   -----END CERTIFICATE REQUEST-----
   ```

2. Copy the certificate signing request from the Agent machine, including the dashes.
3. In Alation, paste the certificate signing request into the provided box under **Certificate Signing Request Output**. Then click the **Next** button.

   New User Experience



Generate Certificate Signing Request (CSR)

Copy and run the below command on the Agent machine to generate a certificate signing request.

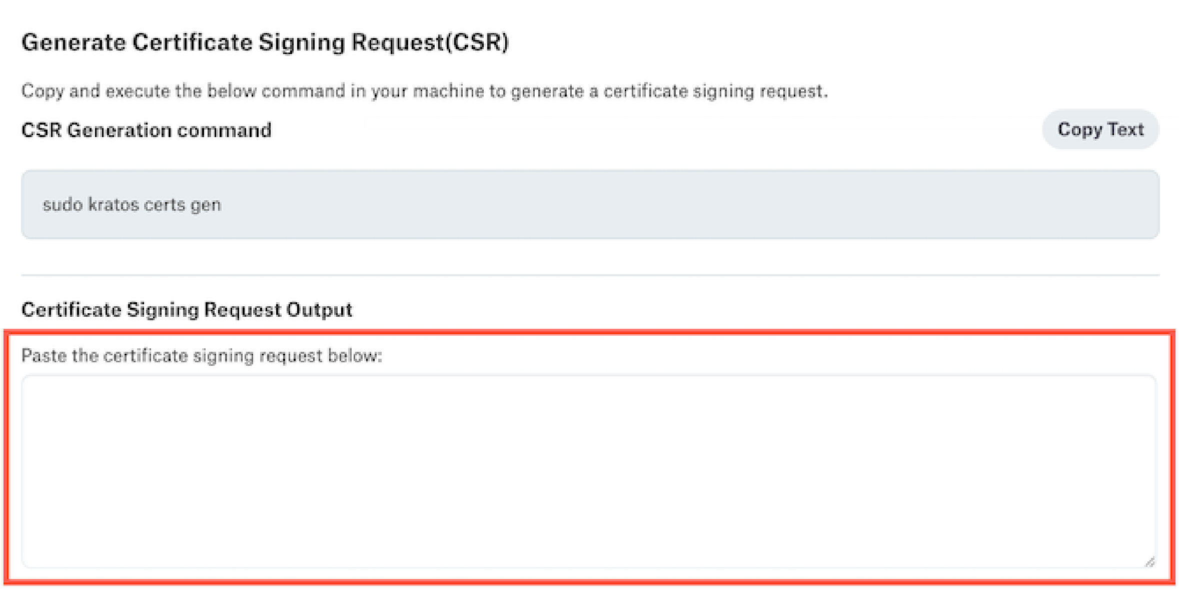
CSR Generation Command

```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

   Classic User Experience



Generate Certificate Signing Request(CSR)

Copy and execute the below command in your machine to generate a certificate signing request.

CSR Generation command

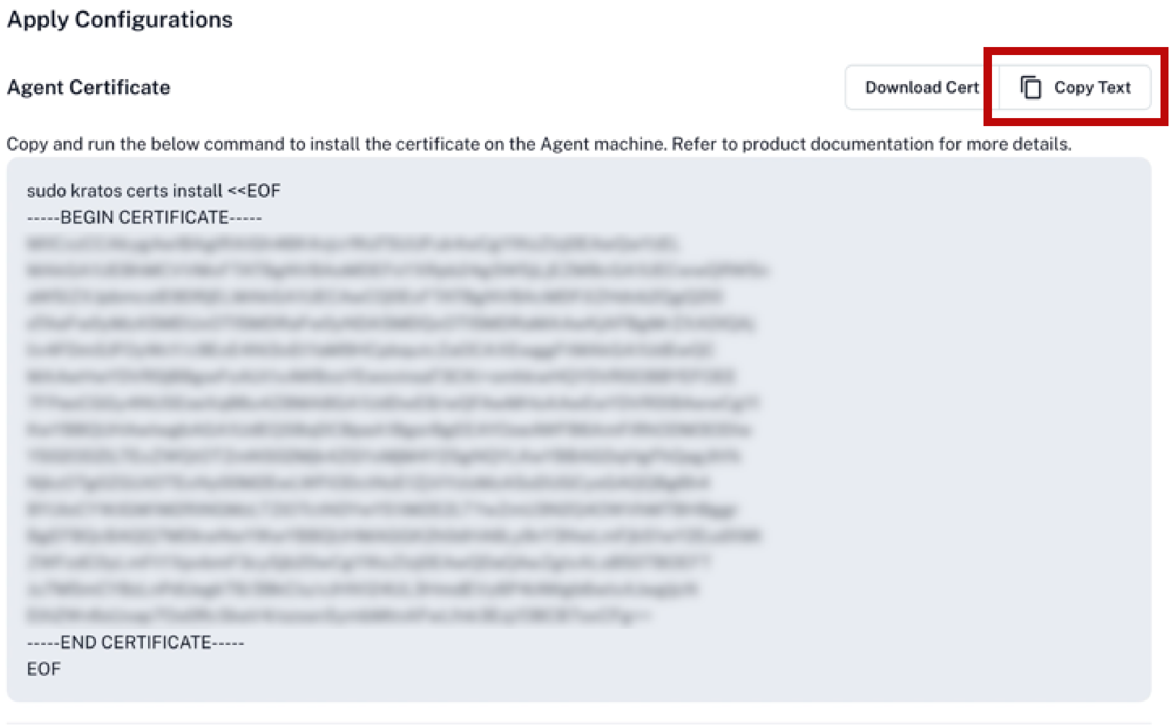
```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

4. Alation will generate two signed certificates—one for the Agent and one root certificate. Copy the provided certificate installation command.

New User Experience



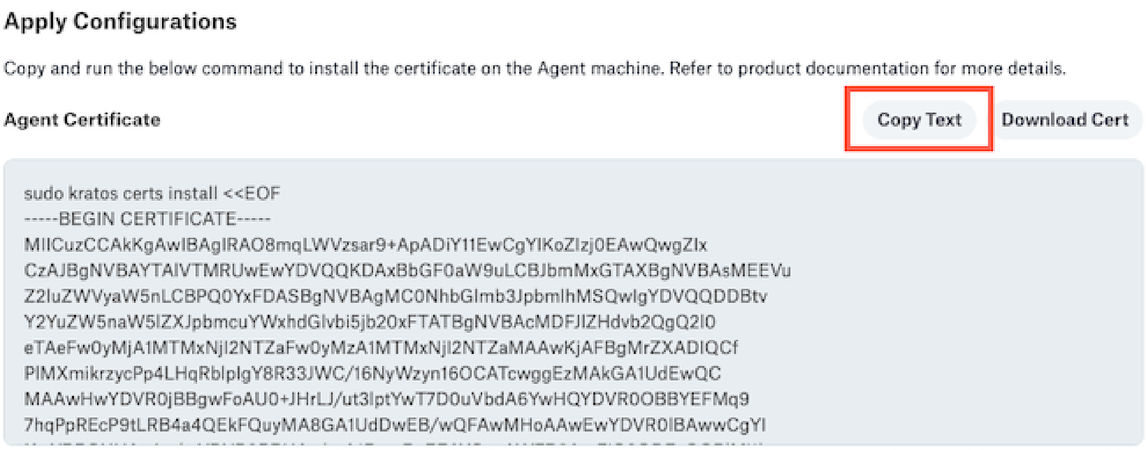
Apply Configurations

Agent Certificate

Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
EOF
```

Classic User Experience



Apply Configurations
Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.
Agent Certificate
Copy Text
Download Cert

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
MIICuzCCAkKgAwIBAgIRAO8mqLWVzsar9+ApADiY11EwCgYIKoZIzj0EAwQwgZIx
CzAJBgNVBAYTAlVTMRUwEwYDVQQKDAxBbGF0aW9uLCBJbmMxGTAXBgNVBAsMEEVu
Z2luZWVyaW5nLCBPQ0YxFDASBgNVBAgMC0NhbGlmb3JpbmlhMSQwIgYDVQQDDBtv
Y2YuZW5naW5lZXJpbmcuYWxhdGlvbi5jb20xFTATBgNVBAcMDFJlZHdvb2QgQ2l0
eTAeFw0yMjA1MTMxNjI2NTZaFw0yMzA1MTMxNjI2NTZaMAAwKjAFBgMrZXADIQCf
PIMXmikrzycPp4LHqRblplgY8R33JWC/16NyWzyn16OCATcwggEzMAkGA1UdEwQC
MAAwHwYDVR0jBBgwFoAU0+JHrLJ/ut3lptYwT7D0uVbdA6YwHQYDVR0OBBYEFMq9
7hqPpREcP9tLRB4a4QEkFQuyMA8GA1UdDwEB/wQFAwMHoAAwEwYDVR0lBAwwCgYI
```

5. On the Agent's host machine, paste the copied certificate command and run it. This installs the certificate.

   Warning: The certificates will automatically expire after one year.

6. Restart the Agent by copying the provided command and running it on the Agent's host machine.

   ```
   sudo systemctl restart hydra
   ```

7. When the Agent has finished restarting, click the **Finish** button in Alation. Check that your Agent has a status of **Connected** in the Agent Dashboard. If it doesn't, check the *Troubleshooting* page.

If the installation was successful, you can now install connectors on your Agent.

Step 5: Install the Authentication Service Add-on (Optional)

If you would like to enable the Alation Agent to integrate directly with AWS Secrets Manager when authenticating requests to your data source, you can install the Authentication Service add-on.

To use this feature, you must meet the following requirements:

- You must be an Alation Cloud Service customer on the cloud-native architecture.
- You must be using *Alation Agent version 1.7.2.4360* or later. For help installing the Alation Agent, see *Install the Alation Agent*.
- To access AWS Secrets Manager using an IAM instance profile:
  - You must be on Alation Cloud Service version 2024.1.4 or later.
  - Your Alation Agent must be installed on an Amazon EC2 instance.
  - You must install *Authentication Service Add-on* version 5.14.0.1882 or later on the Alation Agent.
- To access AWS Secrets Manager using an IAM user's credentials:
  - You must be on Alation Cloud Service version 2024.1.5 or later.
  - You must install *Authentication Service Add-on* version 5.14.0.1968 or later on the Alation Agent.

- You must have a supporting OCF connector installed on the Agent. To find out if a specific connector supports this feature, see the documentation for the specific connector in the /sources/OpenConnectorFramework/index section.

Note: You can use the Native Data Sources API to migrate a data source from an OCF connector that's not on an Alation Agent to an OCF connector that is on an Alation Agent.

To install or update the Authentication Service add-on on an Alation Agent:

1. If you don't have the latest plugin yet, contact Alation Support to request it. The plugin is a Docker image named **auth-service-docker-image-<plugin-version>tar.gz**.

2. If needed, transfer the downloaded file to the Agent's host machine. For example, if you downloaded the plugin file to a Unix-based machine, you could transfer the file using the `scp` command in Terminal:

```
scp /local/path/to/auth-service-docker-image-<plugin-version>.tar.gz <ssh-user>@
<server-address>:/remote/path/to/agent
```

3. On the Agent's host machine, unzip the **.tar.gz** file. Example:

```
gzip -d auth-service-docker-image-<plugin-version>.tar.gz
```

4. Install or update the plugin. To install the plugin from scratch, use this command:

```
sudo kratos addons install auth ./auth-service-docker-image-<plugin-version>.tar
```

To update the plugin, use this command:

```
sudo kratos addons update auth ./auth-service-docker-image-<plugin-version>.tar
```

5. Restart the Agent:

```
sudo systemctl restart hydra
```

6. Check that the plugin is running. It may take about two minutes for the plugin to start up.

```
sudo docker ps
```

In the output of this command, you should see `auth` listed under `IMAGE`, and under `STATUS` it should indicate that the plugin is `Up`. For example:

```
CONTAINER ID   IMAGE                 COMMAND                  CREATED
STATUS                             PORTS
NAMES
00d929b2582b   auth                  "java -Dlog4j.config..."   11 seconds ago   Up
10 seconds                      0.0.0.0:11001->11001/tcp, :::11001->11001/tcp   auth
f80e23b27e2a   application_gateway   "/opt/cag"               11 seconds ago   Up 10
seconds (health: starting)                                                   cag
c8c16128644e   proxy                 "/opt/reverseProxy"      12 seconds ago   Up 11
seconds (health: starting)                                                   proxy
8c3d5cfeb3fd   connector_21          "/opt/entrypoint.sh ..."   12 seconds ago   Up
12 seconds (health: starting)   127.0.0.1:10021->10021/tcp
connector21
c8814bcadc3c   agent                 "/opt/agent"             13 seconds ago   Up 12
seconds (health: starting)   127.0.0.1:8080->8080/tcp                        agent
```

The Authentication Service add-on has now been installed. To troubleshoot the Agent or Authentication Service add-on, see *Troubleshoot the Agent*.

See /sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/index for information on different ways to integrate with AWS Secrets Manager, along with detailed instructions.

4.4.3 Work with the Agent's Certificates

Alation Cloud Service

Alation uses signed certificates to encrypt the communication between your Alation Cloud instance and the Agent. Alation uses two signed certificates—one for the Agent and one root certificate. These certificates will automatically expire after one year.

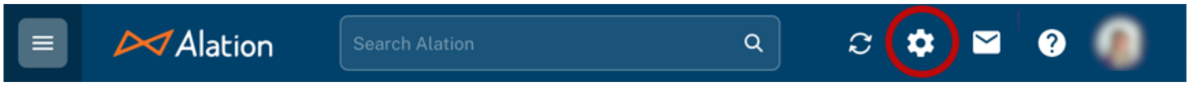
You're in full control of these certificates. You can always view the certificates in Alation. You can revoke them at any time to stop communication between your Alation Cloud instance and the Agent. You can also renew certificates at any time, whether they are current, expired, or revoked.

Navigate to the Agents Dashboard

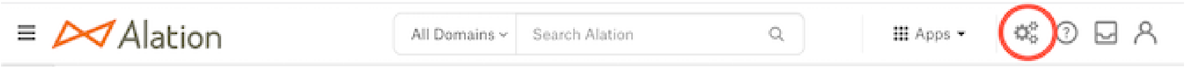
To work with the Agent's certificates, first navigate to the Agents Dashboard:

1. Click on the **Settings** icon in the top right corner.

   New User Experience

   Classic User Experience

2. **New User Experience**

   The **Admin Settings** page appears. Under the **Platform Settings** section, click **Agents**.

   Classic User Experience

   Under the **Server Admin** section, click **Manage Connectors**. Then click the **Agents** tab. The **Agents Dashboard** appears.

View the Certificates' Expiration Date

To view the expiration date of the Agent's certificates:

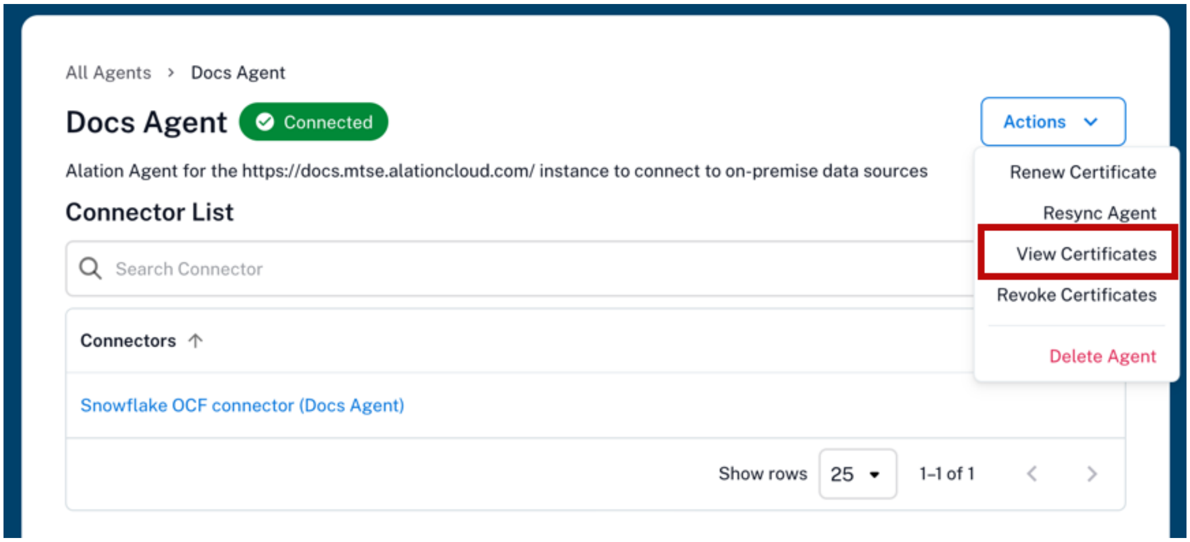
1. Navigate to the *Agents Dashboard*.
2. In the **Certificate Expiration** column, you can see the date on which the certificates will expire. If there is no date, then there are no valid certificates associated with that Agent.

View the Certificates

To view an Agent's certificates:

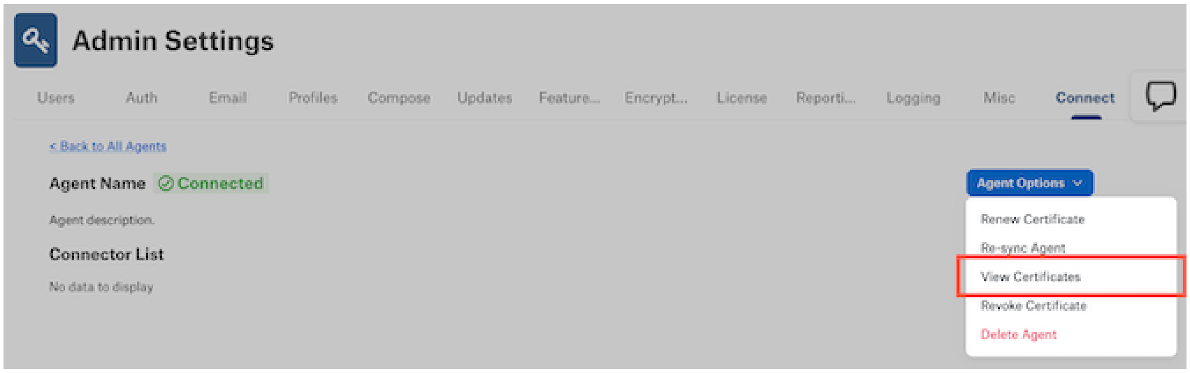
1. Navigate to the *Agents Dashboard*.
2. Click on the name of the Agent. The Agent's dedicated page opens.
3. **New User Experience**

   Click the **Actions** button, then select **View Certificates**.



   Classic User Experience

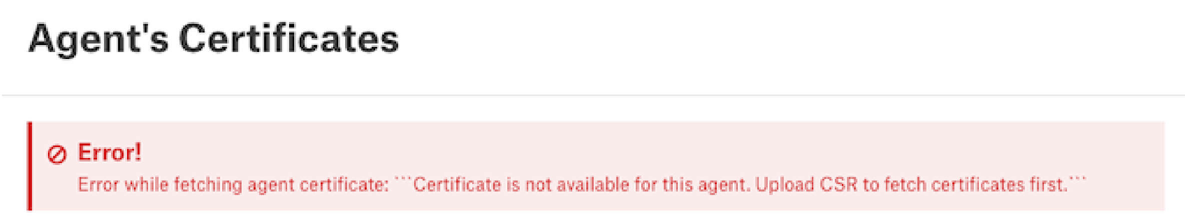
   Click the **Agent Options** button, then select **View Certificates**.



4. A dialog will appear that shows the certificates.

Note: If the certificate has been revoked, you'll see an error message.

Classic User Experience



Agent's Certificates

Error!

Error while fetching agent certificate: ```Certificate is not available for this agent. Upload CSR to fetch certificates first.```

See *Renew the Certificates* to reestablish the connection.

5. Click the **Close** button to exit the dialog.

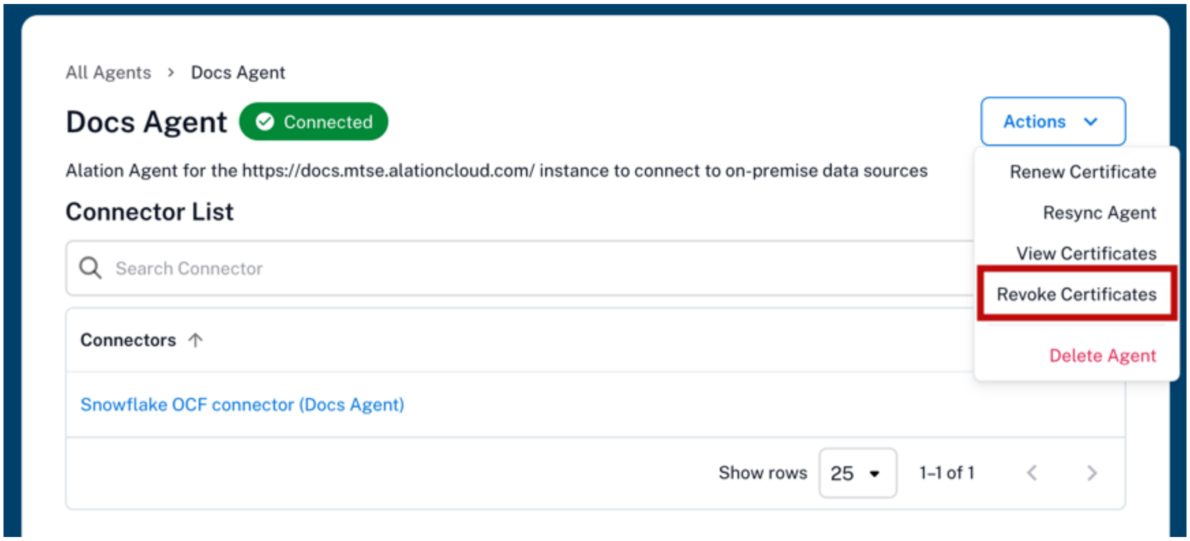
Revoke the Certificates

You can revoke the Agent’s certificates at any time. This stops all communication between the Agent and your Alation Cloud instance.

To revoke an Agent’s certificates:

1. Navigate to the *Agents Dashboard*.
2. Click on the name of the Agent. The Agent’s dedicated page opens.
3. **New User Experience**

   Click the **Actions** button, then select **Revoke Certificates**.



All Agents > Docs Agent

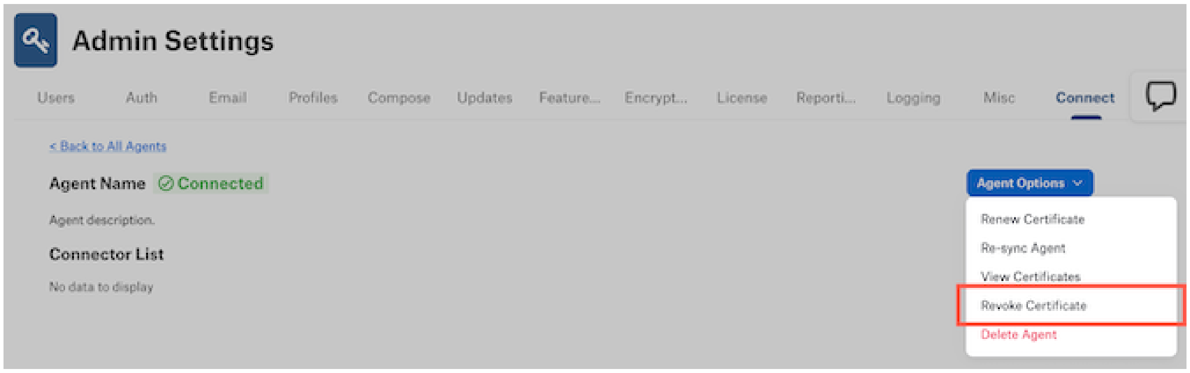
Docs Agent

Alation Agent for the https://docs.mtse.alationcloud.com/ instance to connect to on-premise data sources

Connector List

   Classic User Experience

   Click the **Agent Options** button, then select **Revoke Certificates**.



4. A confirmation dialog appears. Click the **Confirm** button to revoke the certificate.

Important: It may take up to an hour before the certificate is fully revoked, per the Online Certificate Status Protocol (RFC 5019) Section 6. Your Agent may appear to have a **Connected** status until that time.

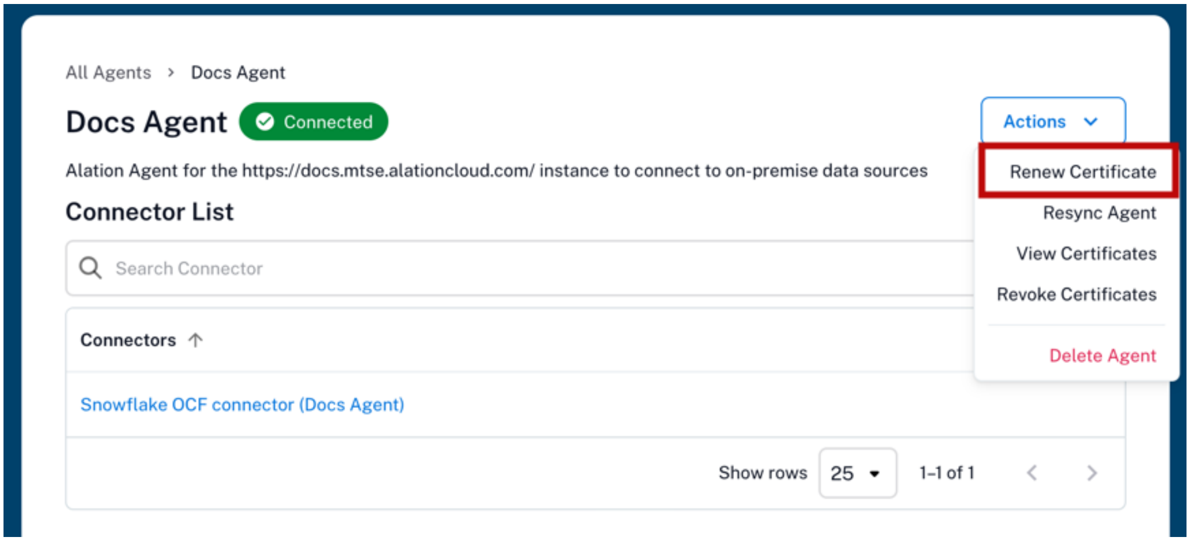
Renew the Certificates

Agent certificates automatically expire after one year. You'll need to renew them on a yearly basis in order to keep using the Agent. You may also need to renew certificates that you have previously revoked.

To renew an Agent's certificates:

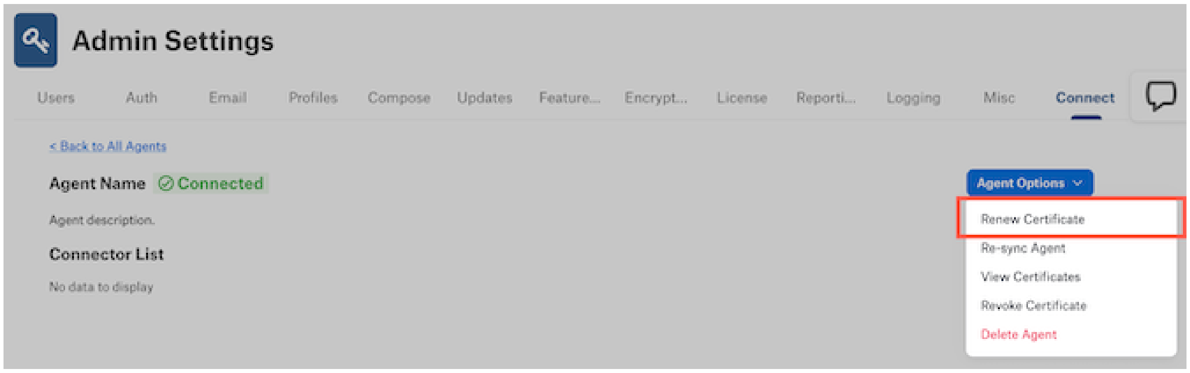
1. Navigate to the *Agents Dashboard*.
2. Click on the name of the Agent. The Agent's dedicated page opens.
3. **New User Experience**

   Click the **Actions** button, then select **Renew Certificate**.



   Classic User Experience

   Click the **Agent Options** button, then select **Renew Certificate**.



4. On the **Generate Certificate Signing Request (CSR)** screen, copy the provided command and run it on the Agent's host machine.

```
sudo kratos certs gen
```

   Since this Agent has already been connected to your Alation Cloud instance in the past, you will get a warning that a key has already been created.

```
Warning! A key for this agent appears to have already been generated
at "/etc/hydra/agent/security/proxy_key.pem". Generating a new key pair
will destroy the existing one.
Continue? [Y|n]
```

   Enter **Y** to continue.

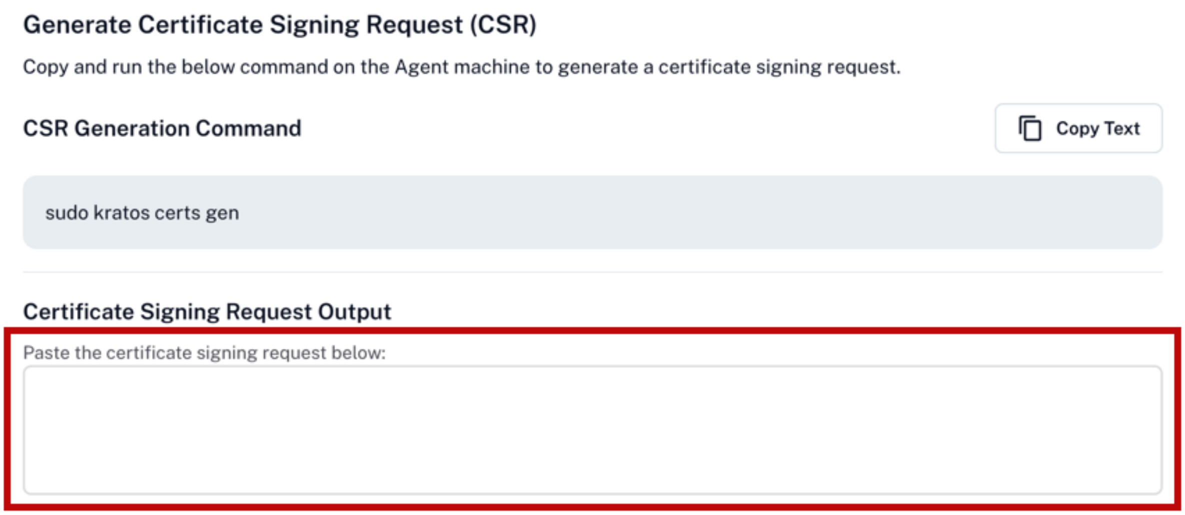
   The command will generate a certificate signing request. Example output:

```
-----BEGIN CERTIFICATE REQUEST-----
<your certificate signing request>
-----END CERTIFICATE REQUEST-----
```

5. Copy the certificate signing request from the Agent machine, including the dashes.

6. In Alation, paste the certificate signing request into the provided box under **Certificate Signing Request Output**. Then click the **Next** button.

   New User Experience



Generate Certificate Signing Request (CSR)

Copy and run the below command on the Agent machine to generate a certificate signing request.

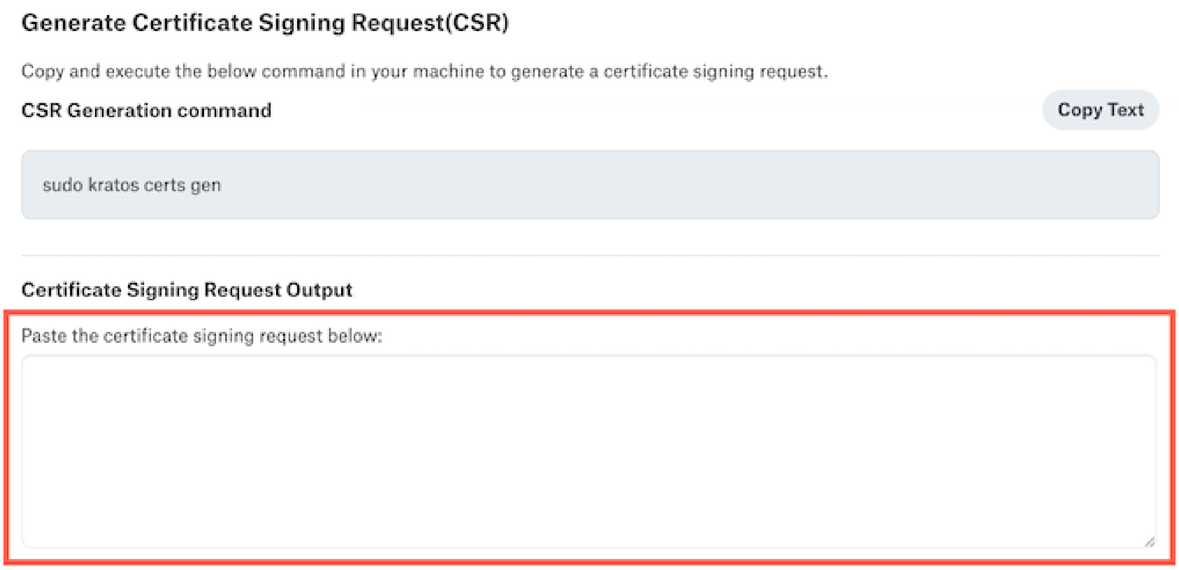
CSR Generation Command

```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

Classic User Experience



Generate Certificate Signing Request(CSR)

Copy and execute the below command in your machine to generate a certificate signing request.

CSR Generation command

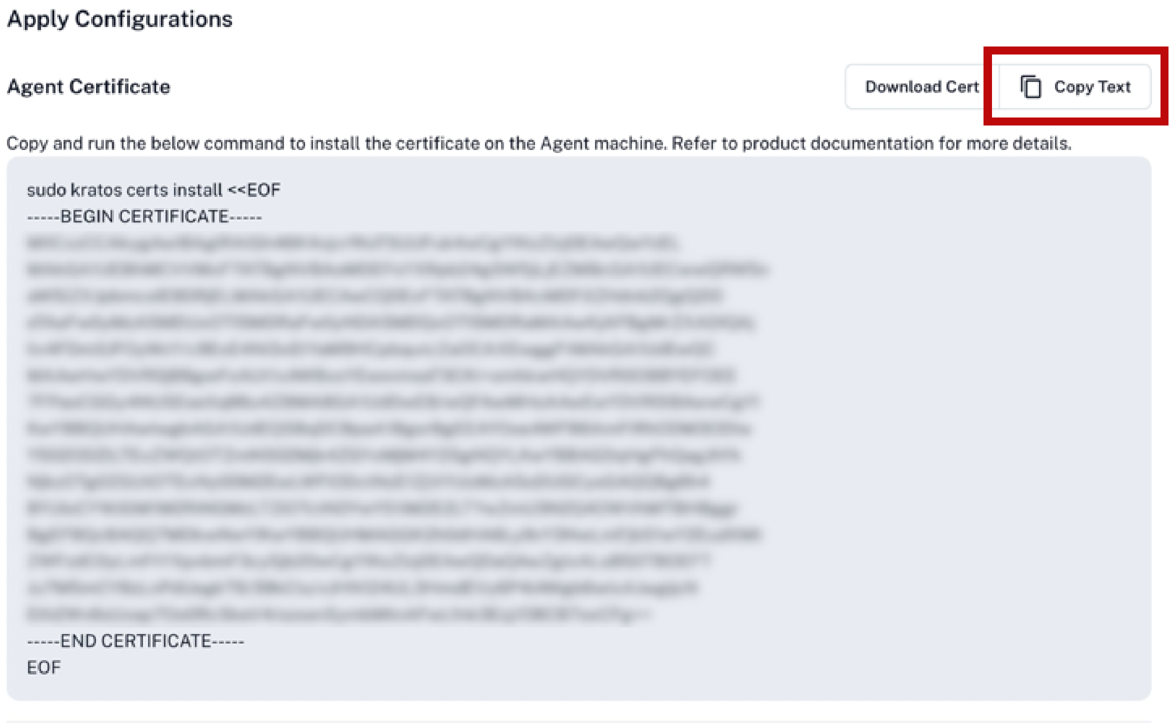
```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

7. Alation will generate two signed certificates—one for the Agent and one root certificate. Copy the provided certificate installation command.

New User Experience



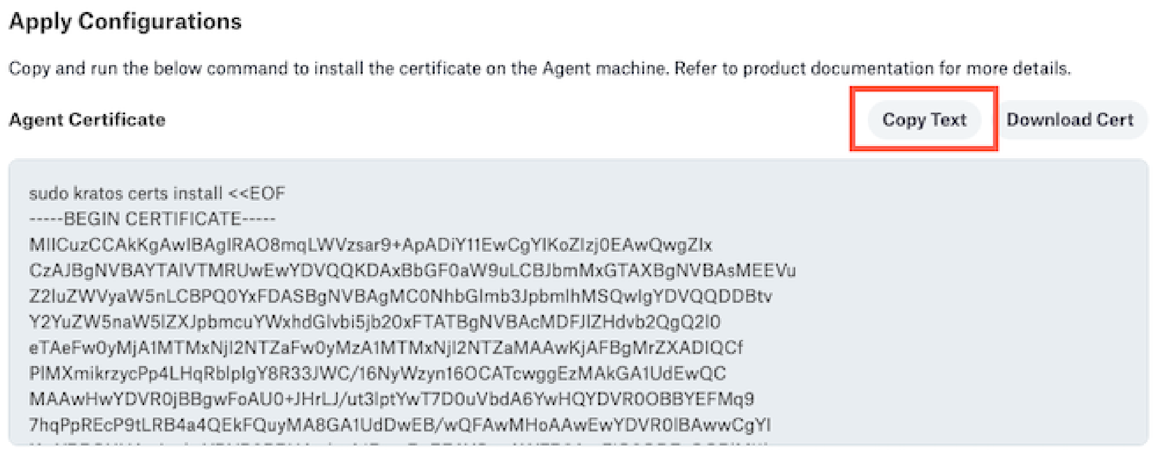
Apply Configurations

Agent Certificate

Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
EOF
```

Classic User Experience



Apply Configurations

Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

Agent Certificate

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
MIICuzCCAkKgAwIBAgIRAO8mqLWVzsar9+ApADiY11EwCgYIKoZIzj0EAwQwgZIx
CzAJBgNVBAYTAlVTMRUwEwYDVQQKDAxBbGF0aW9uLCBJbmMxGTAXBgNVBAsMEEVu
Z2luZWVyaW5nLCBPQ0YxFDASBgNVBAgMC0NhbGlmb3JpbmlhMSQwIgYDVQQDDBtv
Y2YuZW5naW5lZXJpbmcuYWxhdGlvbi5jb20xFTATBgNVBAcMDFJlZHdvb2QgQ2l0
eTAeFw0yMjA1MTMxNjI2NTZaFw0yMzA1MTMxNjI2NTZaMAAwKjAFBgMrZXADIQCf
PlMXmikrzycPp4LHqRblplgY8R33JWC/16NyWzyn16OCATcwggEzMAkGA1UdEwQC
MAAwHwYDVR0jBBgwFoAU0+JHrLJ/ut3lptYwT7D0uVbdA6YwHQYDVR0OBBYEFMq9
7hqPpREcP9tLRB4a4QEkFQuyMA8GA1UdDwEB/wQFAwMHoAAwEwYDVR0lBAwwCgYI
```

8. On the Agent's host machine, paste the copied certificate command and run it. This installs the certificate.

9. Restart the Agent by copying the provided command and running it on the Agent's host machine.

```
sudo systemctl restart hydra
```

10. When the Agent has finished restarting, click the **Finish** button in Alation. Check that your Agent has a status of **Connected** in the Agent Dashboard. If it doesn't, check the *Troubleshooting* page.

Warning: The certificates will automatically expire after one year.

4.4.4 Upgrade the Agent

Alation Cloud Service

To upgrade an Alation Agent (Agent) installation to a newer version:

1. On the Agent host machine, check the installed Agent's version by running:

```
hydra version
```

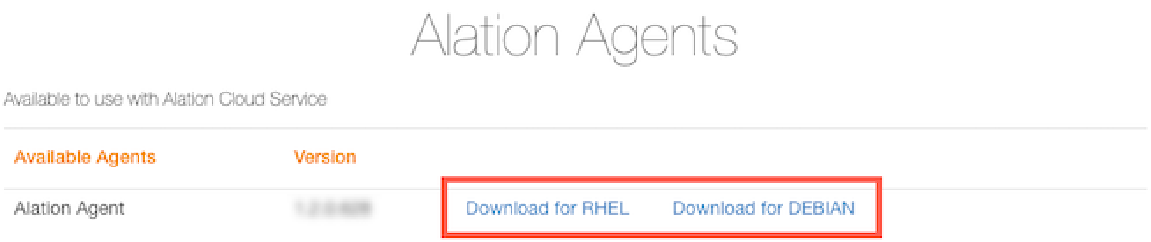
The version number will be in the first line of the output.

2. Go to the Alation Customer Portal. If prompted, log in.

3. If a newer version of the Agent is available in the **Version** column of the Alation Customer Portal, proceed with the upgrade.

4. In the Alation Customer Portal, select the latest available version for the desired operating system:

   - **RHEL** for Red Hat-based systems
   - **DEBIAN** for Debian-based systems



Alation Agents

Available to use with Alation Cloud Service

Available Agents	Version		
Alation Agent	[redacted]	Download for RHEL	Download for DEBIAN

The Agent will download to your computer as a tar.gz file named **ocf-agent-<agent-version>-<operating-system>.tar.gz**.

5. If needed, transfer the downloaded file to the Agent's host machine. For example, if you downloaded the Agent file to a Unix-based machine, you could transfer the file using the `scp` command in Terminal:

```
scp /local/path/to/ocf-agent-<agent-version>-<operating-system>.tar.gz <ssh-user>@
<server-address>:/remote/path/to/ocf-agent
```

Important: If you already have an **ocf-agent** directory on the Agent machine, remove or rename it so its old files won't interfere with the current process.

6. On the Agent's host machine, extract the **.tar.gz** file. Example:

```
tar -xf ocf-agent-<agent-version>-<operating-system>.tar.gz
```

The Agent installation files are extracted into an **ocf-agent** directory.

7. Change into the ocf-agent directory.

```
cd ocf-agent
```

Then check the name of the installation files.

```
ls
```

There should be two files. One for the Alation Container Service (Docker) named something like **alation-container-service-<version>.deb** or **alation-container-service-<version>.rpm**, and one for the Agent named something like **ocf-agent-<version>.deb** or **ocf-agent-<version>.rpm**.

Warning: Compatibility between Alation Container Service (Docker) and Alation Agent

If you do not upgrade the Alation Container Service (Docker) when you upgrade your Alation Agent, you may encounter compatibility issues due to a version mismatch between the Docker Engine API and the Alation Agent.

8. Before you upgrade the Alation Agent, run one of the following commands to upgrade the Alation Container Service, replacing "<alation-container-service-installer-file>" with the file name of the Alation Container Service installer:

On a Debian-based machine:

```
sudo dpkg --install <alation-container-service-installer-file>
```

On a Red Hat-based machine:

```
sudo rpm -Uvh <alation-container-service-installer-file>
```

9. Run one of the following commands, replacing "<agent-install-file>" with the file name of the Agent installer you downloaded.

   On a Debian-based machine:

   ```
   sudo dpkg --install <agent-install-file>
   ```

   On a Red Hat-based machine:

   ```
   sudo rpm -Uvh <agent-install-file>
   ```

10. If you're upgrading the Agent as part of an upgrade to Alation's cloud native architecture, you may also need to update the Agent configuration file. See *Update the Agent's Address Configuration*.

11. Restart the Agent by copying the provided command and running it on the Agent's host machine.

    ```
    sudo systemctl restart hydra
    ```

    The upgrade process is complete when the Agent is done restarting.

12. Verify the upgraded Agent's version by running:

    ```
    hydra version
    ```

    The version number will be in the first line of the output.

4.4.5 Update the Agent's Address Configuration

Alation Cloud Service

You may need to update the Agent's address configuration if the Agent is in a disconnected status. This may happen if the Agent was set up incorrectly or if you're an Alation Cloud Service customer who's been upgraded to the cloud native architecture (available starting in 2022.4).

To update the Agent's address configuration:

1. Look up the Alation Cloud Service connectivity endpoint for your region in the following table.

Geography	Location	Agent Connectivity Endpoint
Africa, Europe, & Middle East	Frankfurt	ocf.euc1.eu.alationcloud.com
	Dublin	ocf.euw1.eu.alationcloud.com
Americas	Montreal	ocf.cac1.ca.alationcloud.com
	Virginia	ocf.use1.alationcloud.com
	Oregon	ocf.usw2.alationcloud.com
Asia Pacific	Singapore	ocf.apse1.ap.alationcloud.com
	Sydney	ocf.apse2.ap.alationcloud.com
	Tokyo	ocf.apne1.ap.alationcloud.com

2. If your organization uses a Web Application Firewall (WAF), inform your firewall admin to allow the Alation Cloud Service connectivity endpoint to pass through.

3. The Agent configuration file is located on the Agent host machine at **/etc/hydra/hydra.toml**. Edit the file using your preferred text editor. You may need to use sudo privileges.

4. In **hydra.toml**, look for the `address` line. Replace the address value inside the quotation marks with the Alation Cloud Service connectivity endpoint you obtained earlier. If the address is already correct, you don't need to do anything else.

5. Restart the agent by running the following command:

   ```
   sudo hydra restart
   ```

6. In Alation, return to the Agents Dashboard and verify that the Agent is now connected to Alation.

4.4.6 Authentication Service Add-on

The Authentication Service add-on for the Alation Agent is an optional feature that enables you to integrate the Alation Agent with AWS Secrets Manager for authenticating with your on-premises data sources. With this method, your data source credentials never have to leave your network. For more information on how this works and other options you have, see /sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/index.

To use this feature, you must meet the following requirements:

- You must be an Alation Cloud Service customer on the cloud-native architecture.
- You must be using *Alation Agent version 1.7.2.4360* or later. For help installing the Alation Agent, see *Install the Alation Agent*.
- To access AWS Secrets Manager using an IAM instance profile:
  - You must be on Alation Cloud Service version 2024.1.4 or later.
  - Your Alation Agent must be installed on an Amazon EC2 instance.
  - You must install *Authentication Service Add-on* version 5.14.0.1882 or later on the Alation Agent.
- To access AWS Secrets Manager using an IAM user's credentials:
  - You must be on Alation Cloud Service version 2024.1.5 or later.
  - You must install *Authentication Service Add-on* version 5.14.0.1968 or later on the Alation Agent.
- You must have a supporting OCF connector installed on the Agent. To find out if a specific connector supports this feature, see the documentation for the specific connector in the /sources/OpenConnectorFramework/index section.

Note: You can use the Native Data Sources API to migrate a data source from an OCF connector that's not on an Alation Agent to an OCF connector that is on an Alation Agent.

Authentication Service Add-on Release Notes

Release 5.14.0.1968

Released August 1, 2024

Alation Cloud Service customer on the cloud-native architecture only

The Authentication Service add-on now offers the ability to connect to AWS Secrets Manager using IAM user credentials. This allows you to use the Authentication Service add-on in non-AWS environments. To use this feature, you must be an Alation Cloud Service customer on the cloud-native architecture who has upgraded to Alation 2024.1.5. See

/sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/AccessSecretsMan
for more information.

Release 5.14.0.1882

Released July 4, 2024

Alation Cloud Service customer on the cloud-native architecture only

This is the initial release of the Authentication Service add-on for the Alation Agent. In the initial release, integrating with AWS Secrets Manager using an IAM instance profile is supported. To use this feature, you must be an Alation Cloud Service customer on the cloud-native architecture who has upgraded to Alation 2024.1.4. See /sources/OpenConnectorFramework/ConfigureSecretsforOCFConnectors/ConfigureAWSSecretsManager/AccessSecretsMan
for more information.

Note: The Authentication Service add-on has been used internally in Alation Cloud Service itself for some time now. That's why the version number for the initial external release is already so high.

Install or Update the Authentication Service Add-on on an Alation Agent

To install or update the Authentication Service add-on on an Alation Agent:

1. If you don't have the latest plugin yet, contact Alation Support to request it. The plugin is a Docker image named **auth-service-docker-image-<plugin-version>tar.gz**.

2. If needed, transfer the downloaded file to the Agent's host machine. For example, if you downloaded the plugin file to a Unix-based machine, you could transfer the file using the `scp` command in Terminal:

   ```
   scp /local/path/to/auth-service-docker-image-<plugin-version>.tar.gz <ssh-user>@
   <server-address>:/remote/path/to/agent
   ```

3. On the Agent's host machine, unzip the **.tar.gz** file. Example:

   ```
   gzip -d auth-service-docker-image-<plugin-version>.tar.gz
   ```

4. Install or update the plugin. To install the plugin from scratch, use this command:

   ```
   sudo kratos addons install auth ./auth-service-docker-image-<plugin-version>.tar
   ```

   To update the plugin, use this command:

   ```
   sudo kratos addons update auth ./auth-service-docker-image-<plugin-version>.tar
   ```

5. Restart the Agent:

   ```
   sudo systemctl restart hydra
   ```

6. Check that the plugin is running. It may take about two minutes for the plugin to start up.

   ```
   sudo docker ps
   ```

   In the output of this command, you should see `auth` listed under `IMAGE`, and under `STATUS` it should indicate that the plugin is `Up`. For example:

```
CONTAINER ID   IMAGE                 COMMAND                  CREATED
STATUS                             PORTS
NAMES
00d929b2582b   auth                 "java -Dlog4j.config..."   11 seconds ago   Up
10 seconds                      0.0.0.0:11001->11001/tcp, :::11001->11001/tcp   auth
f80e23b27e2a   application_gateway   "/opt/cag"               11 seconds ago   Up 10
seconds (health: starting)                                                   cag
c8c16128644e   proxy                 "/opt/reverseProxy"      12 seconds ago   Up 11
seconds (health: starting)                                                   proxy
8c3d5cfeb3fd   connector_21          "/opt/entrypoint.sh ..."   12 seconds ago   Up
12 seconds (health: starting)   127.0.0.1:10021->10021/tcp
connector21
c8814bcadc3c   agent                 "/opt/agent"             13 seconds ago   Up 12
seconds (health: starting)   127.0.0.1:8080->8080/tcp                        agent
```

The Authentication Service add-on has now been installed. To troubleshoot the Agent or Authentication Service add-on, see *Troubleshoot the Agent*.

Check the Authentication Service Add-on's Status

First log into the machine where the Alation Agent is running, then run the following command:

```
sudo docker ps
```

Stop the Authentication Service Add-on

To stop the Authentication Service add-on, you must stop the entire Agent. First log into the machine where the Alation Agent is running, then run the following command:

```
sudo systemctl stop hydra
```

4.4.7 Delete and Reconnect the Agent in Alation

Alation Cloud Service

Delete the Agent from Alation

You can delete an Agent from the Agents Dashboard in Alation at any time. This will have the following effects:

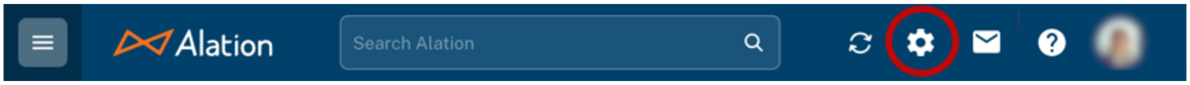
- The Agent is removed from your Agents Dashboard in Alation.
- All connectors you have installed on the Agent will be deleted from the Agent. The data sources will still appear in Alation, but the connection to your physical data source will be broken. You'll no longer be able to use the old data source in Alation to conduct metadata extraction or other operations. If you reinstall the connector, you can add the data source to Alation again, but it will be considered a separate data source from the old one. You will have to rerun metadata extraction again on this new data source.
- The certificate for the Agent is revoked. The connection is broken between your Alation Cloud instance and the Agent software installed on your network.

- The Agent software remains on the host machine where you installed it (unless it has been removed or uninstalled separately). You can *reconnect* it later, if desired.

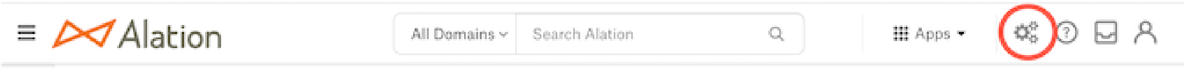
To delete an Agent from Alation:

1. Click on the **Settings** icon in the top right corner.

   New User Experience

   Classic User Experience

2. **New User Experience**

   The **Admin Settings** page appears. Under the **Platform Settings** section, click **Agents**.

   Classic User Experience

   Under the **Server Admin** section, click **Manage Connectors**. Then click the **Agents** tab. The **Agents Dashboard** appears.

3. Click on the name of the Agent. The Agent's dedicated page opens.

4. **New User Experience**

   Click the **Actions** button, then select **Delete Agent**. A confirmation message appears.

   Classic User Experience

   Click the **Agent Options** button, then select **Delete Agent**. A confirmation message appears.

5. Click the **Confirm** button to delete the Agent. A success message appears.

6. Click the **Close** button. You will be returned to the Agents Dashboard. The Agent will no longer be listed.

The Agent software that you installed on your network is unaffected by this procedure, but it will now be unable to connect to your Alation Cloud instance. To reconnect your Agent to your Alation Cloud instance, see *Reconnect an Installed Agent to Alation*. To uninstall the Agent from your network, see *Uninstall and Reinstall the Agent Software*.

Reconnect an Installed Agent to Alation

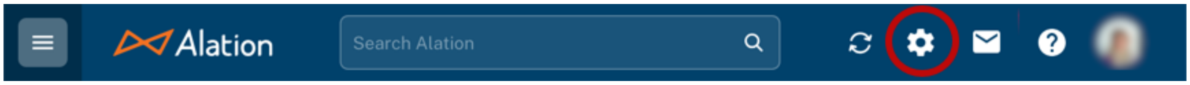
If you have deleted an Agent from the Agent Dashboard in Alation and the Agent software is still running on your network, you can reconnect the installed Agent to your Alation Cloud instance. Before reconnecting the Agent, check the *Alation Cloud Service Compatibility* to see if a newer Agent is available for your Alation Cloud version. If so, upgrade the Agent first.

Step 1: Navigate to the Agent Dashboard

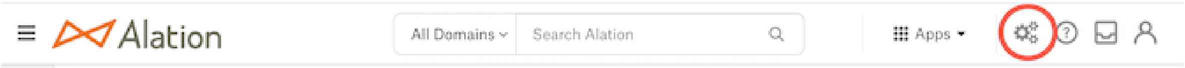
You must have the Server Admin role in Alation to complete these steps.

1. Click on the **Settings** icon in the top right corner.

   New User Experience

   Classic User Experience

2. **New User Experience**

   The **Admin Settings** page appears. Under the **Platform Settings** section, click **Agents**.

   Classic User Experience

   Under the **Server Admin** section, click **Manage Connectors**. Then click the **Agents** tab. The **Agents Dashboard** appears.

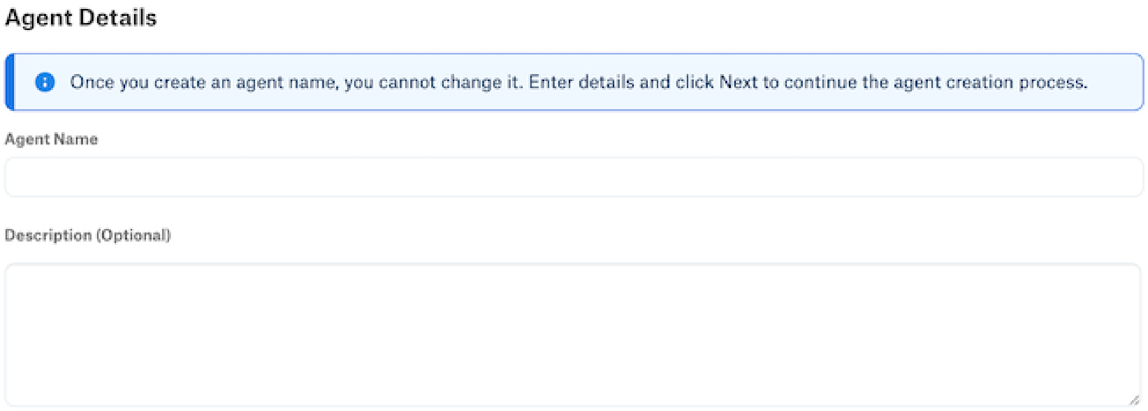
3. Click the **Add New Agent** button. The **Add New Agent** dialog will appear.

4. Click the **Next** button.

Important: Do not follow the installation instructions on the **Install Agent** screen. You do not need to install the Agent again, because it's already installed and running on your network.

Step 2: Name Your Agent

1. In Alation, enter a name for the Agent. This name can't be changed, so choose carefully.



Agent Details

Once you create an agent name, you cannot change it. Enter details and click Next to continue the agent creation process.

Agent Name

Description (Optional)

Note: The Agent's name is used to identify connectors that you install on this Agent. When you install a new connector or add a new data source and link it to your Agent, you'll see the Agent name added to the end of the connector name.

2. *(Optional)* Enter a description of the Agent. This appears on the Agent's detail page. The description can't be changed later.
3. Click the **Next** button, then confirm the name you chose.

Step 3: Generate Encryption Certificates

Alation uses signed certificates to encrypt the communication between Alation and the Agent.

1. On the **Generate Certificate Signing Request (CSR)** screen, copy the provided command and run it on the Agent's host machine.

   ```
   sudo kratos certs gen
   ```

   Since this Agent has already been connected to your Alation Cloud instance in the past, you will get a warning that a key has already been created.

   ```
   Warning! A key for this agent appears to have already been generated
   at "/etc/hydra/agent/security/proxy_key.pem". Generating a new key pair
   will destroy the existing one.
   Continue? [Y|n]
   ```

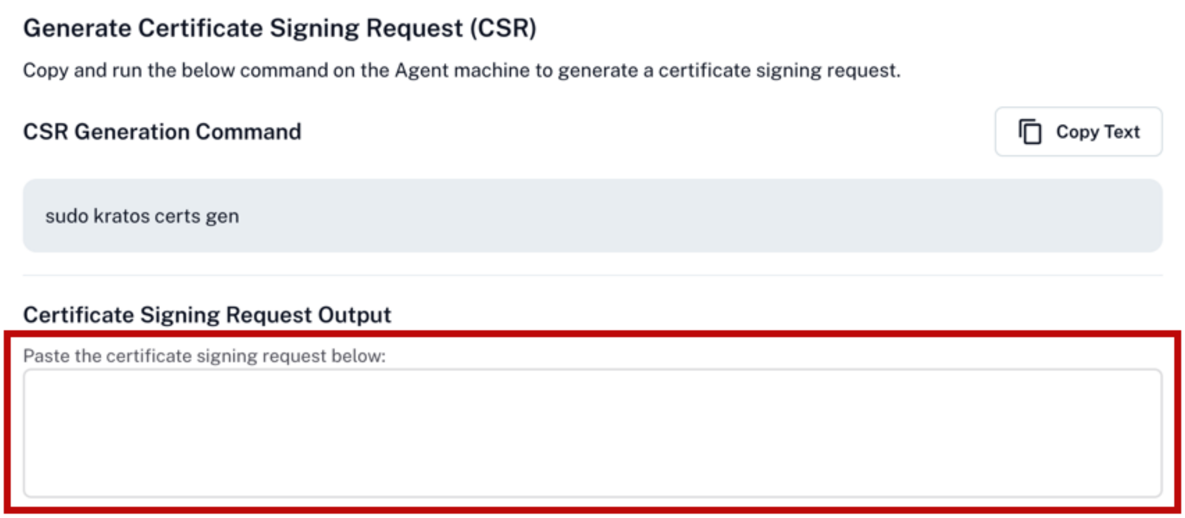
   Enter **Y** to continue.

   The command will generate a certificate signing request. Example output:

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   <your certificate signing request>
   -----END CERTIFICATE REQUEST-----
   ```

2. Copy the certificate signing request from the Agent machine, including the dashes.
3. In Alation, paste the certificate signing request into the provided box under **Certificate Signing Request Output**. Then click the **Next** button.

   New User Experience



Generate Certificate Signing Request (CSR)

Copy and run the below command on the Agent machine to generate a certificate signing request.

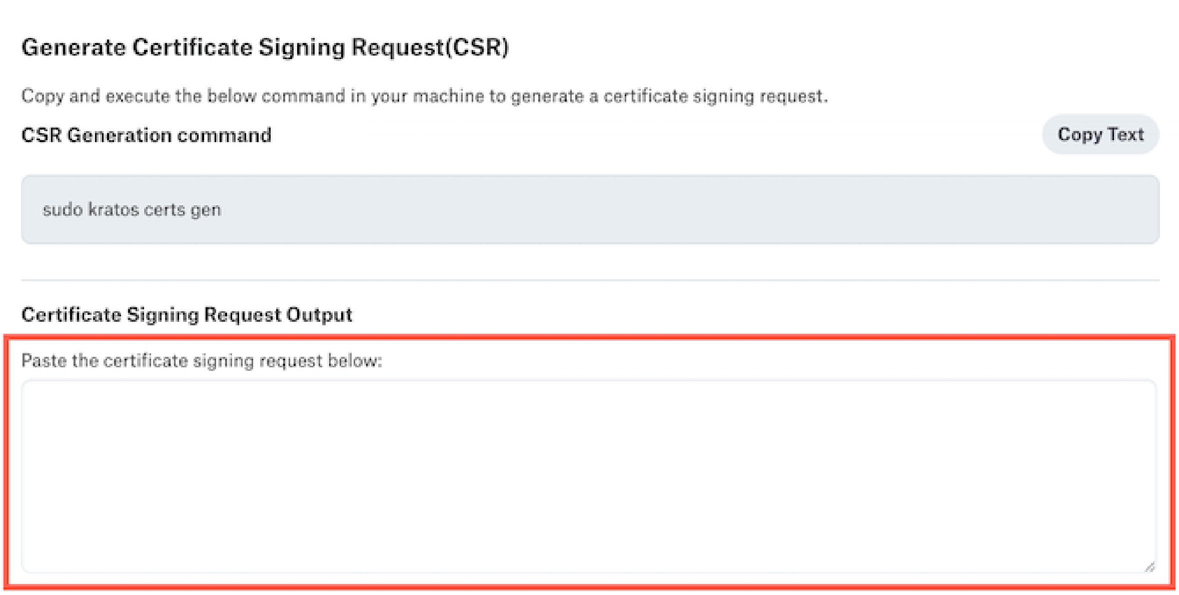
CSR Generation Command

```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

   Classic User Experience



Generate Certificate Signing Request(CSR)

Copy and execute the below command in your machine to generate a certificate signing request.

CSR Generation command

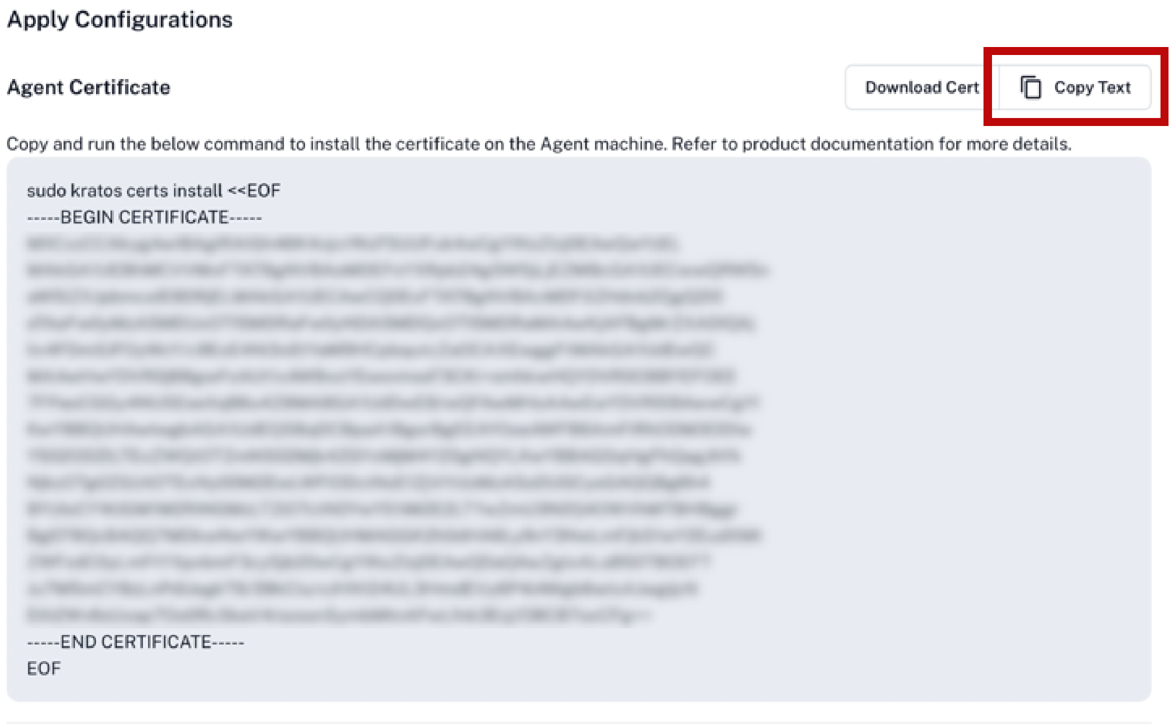
```
sudo kratos certs gen
```

Certificate Signing Request Output

Paste the certificate signing request below:

4. Alation will generate two signed certificates—one for the Agent and one root certificate. Copy the provided certificate installation command.

New User Experience



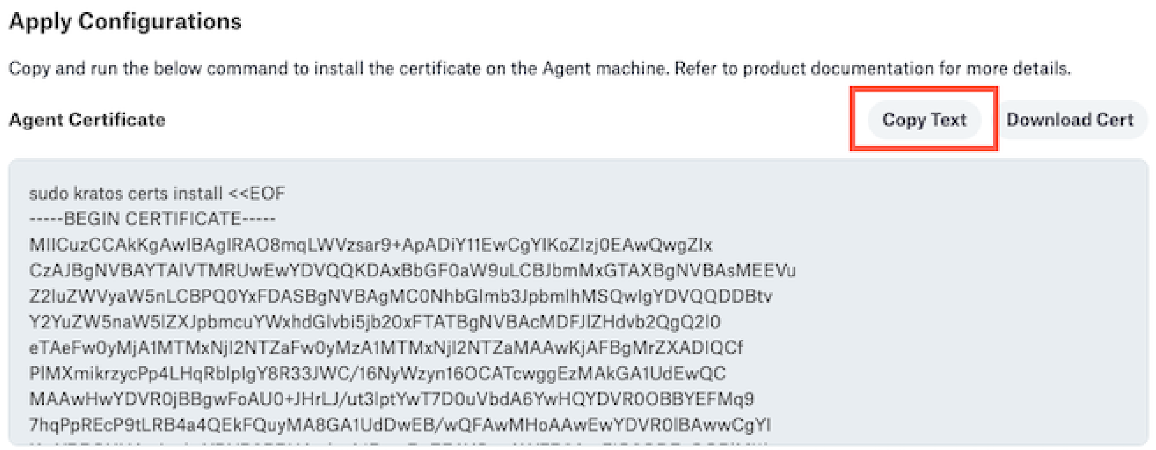
Apply Configurations

Agent Certificate

Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
[illegible]
-----END CERTIFICATE-----
EOF
```

Classic User Experience



Apply Configurations

Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

Agent Certificate

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
MIICuzCCAkKgAwIBAgIRAO8mqLWVzsar9+ApADiY11EwCgYIKoZIzj0EAwQwgZIx
CzAJBgNVBAYTAlVTMRUwEwYDVQQKDAxBbGF0aW9uLCBJbmMxGTAXBgNVBAsMEEVu
Z2luZWVyaW5nLCBPQ0YxFDASBgNVBAgMC0NhbGlmb3JpbmlhMSQwIgYDVQQDDBtv
Y2YuZW5naW5lZXJpbmcuYWxhdGlvbi5jb20xFTATBgNVBAcMDFJlZHdvb2QgQ2l0
eTAeFw0yMjA1MTMxNjI2NTZaFw0yMzA1MTMxNjI2NTZaMAAwKjAFBgMrZXADIQCf
PlMXmikrzycPp4LHqRblplgY8R33JWC/16NyWzyn16OCATcwggEzMAkGA1UdEwQC
MAAwHwYDVR0jBBgwFoAU0+JHrLJ/ut3lptYwT7D0uVbdA6YwHQYDVR0OBBYEFMq9
7hqPpREcP9tLRB4a4QEkFQuyMA8GA1UdDwEB/wQFAwMHoAAwEwYDVR0lBAwwCgYI
```

5. On the Agent's host machine, paste the copied certificate command and run it. This installs the certificate.

6. Restart the Agent by copying the provided command and running it on the Agent's host machine.

   ```
   sudo systemctl restart hydra
   ```

7. When the Agent has finished restarting, click the **Finish** button in Alation. Check that your Agent has a status of **Connected** in the Agent Dashboard. If it doesn't, check the *Troubleshooting* page.

If the installation was successful, you can now install connectors on your Agent.

4.4.8 Uninstall and Reinstall the Agent Software

Alation Cloud Service

Uninstall the Agent

To uninstall an Agent from your network, run the following commands on the Agent's host machine.

Red Hat-Based

Run these two commands in turn.

```
sudo yum remove alation-container-service
```

```
sudo yum remove alation-hydra
```

Debian-Based

Run these two commands in turn.

```
sudo apt-get remove alation-hydra
```

```
sudo apt-get remove alation-container-service
```

Or run these two commands in turn.

```
sudo dpkg --remove alation-hydra
```

```
sudo dpkg --remove alation-container-service
```

After you uninstall an Agent, the corresponding Agent entry on the **Agents Dashboard** in Alation will show as disconnected. To delete the Agent entry from the **Agents Dashboard**, see *Deleting the Agent from Alation*. To reinstall an Agent on your network and connect it to an existing Agent entry in Alation, see below.

Reinstall an Agent and Reconnect to Alation

In some cases, you may have an Agent listed on the Agents Dashboard in Alation, but the Agent software that you had installed inside your network is no longer there. For example, the Agent's host machine may have gone down, or the Agent software may have been uninstalled or deleted.

If this happens, you can install a new copy of the Agent on your network and reconnect it to the Agent entry in Alation. Once the connection has been restored, any connectors you had previously installed on your old Agent will automatically be reinstalled on the new Agent.

Step 1: Prepare for the Installation

Before you can install the Agent, you must:

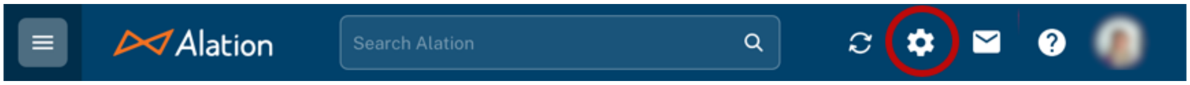
1. Provision a Linux host to install the Agent on. This can be a physical or virtual machine. Do not run other software on this machine—only the Agent should be installed. See *Agent System Requirements* for details.
2. Get access to Alation's Customer Portal. If you don't have access or aren't sure how to access it, contact your account manager.
3. Have the Server Admin role in Alation.

Step 2: Navigate to the Agent Dashboard

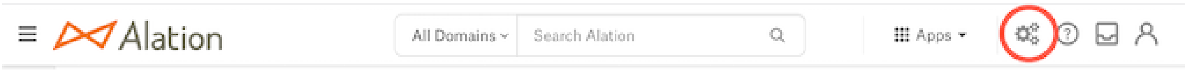
First ensure you have completed the prerequisites in the prior step. You must have the Server Admin role in Alation to complete the remaining steps.

1. Click on the **Settings** icon in the top right corner.

   New User Experience

   Classic User Experience



2. **New User Experience**

   The **Admin Settings** page appears. Under the **Platform Settings** section, click **Agents**.

   Classic User Experience

   Under the **Server Admin** section, click **Manage Connectors**. Then click the **Agents** tab. The **Agents Dashboard** appears.

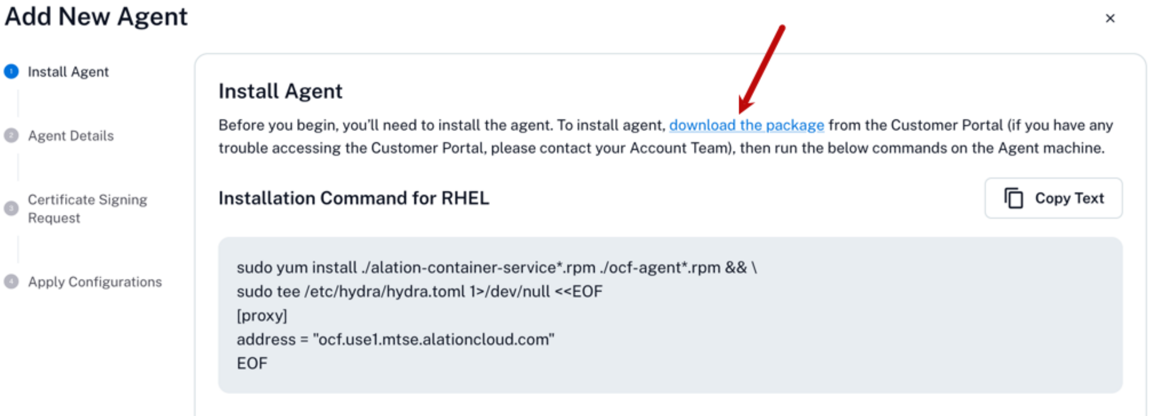
3. Click the **Add New Agent** button. The **Add New Agent** dialog will appear.

> **Note:** You will only need to use the first step in the **Add New Agent** process. This provides you the information needed to install the Agent. Do not click the **Next** button.

Step 3: Download and Run Installation Script

1. In the **Add New Agent** dialog, click the **download the package** link to open the Alation Customer Portal.

   New User Experience



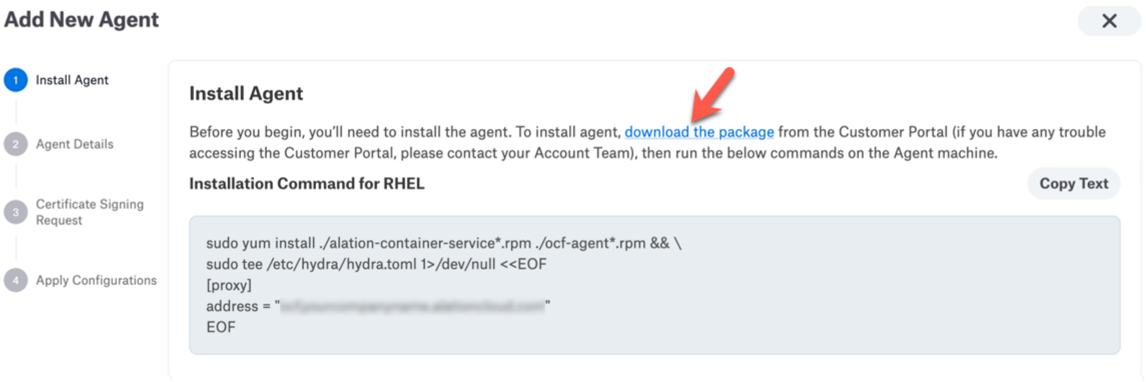
Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "ocf.use1.mtse.alationcloud.com"
EOF
```

   Classic User Experience



Install Agent

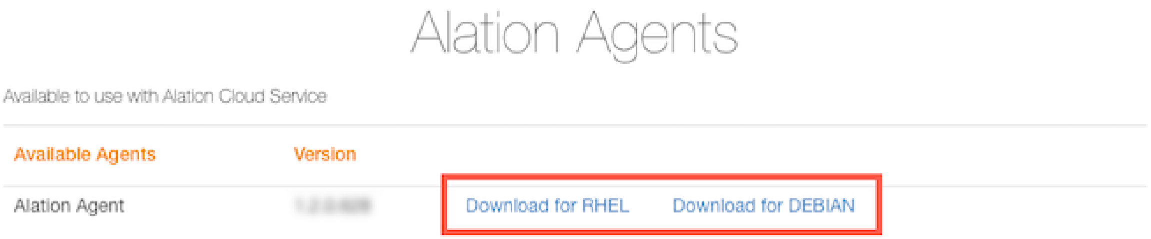
Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

2. In the Alation Customer Portal, select the latest available version for the desired operating system:

- **RHEL** for Red Hat-based systems
- **DEBIAN** for Debian-based systems



Alation Agents

Available to use with Alation Cloud Service

Available Agents	Version		
Alation Agent	[illegible]	Download for RHEL	Download for DEBIAN

The Agent will download to your computer as a tar.gz file named **ocf-agent-<agent-version>-<operating-system>.tar.gz**.

3. If needed, transfer the downloaded file to the Agent's host machine. For example, if you downloaded the Agent file to a Unix-based machine, you could transfer the file using the `scp` command in Terminal:

```
scp /local/path/to/ocf-agent-<agent-version>-<operating-system>.tar.gz <ssh-user>@
<server-address>:/remote/path/to/ocf-agent
```

Important: If you already have an **ocf-agent** directory on the Agent machine, remove or rename it so its old files won't interfere with the current process.

4. On the Agent's host machine, extract the **.tar.gz** file. Example:

```
tar -xf ocf-agent-<agent-version>-<operating-system>.tar.gz
```

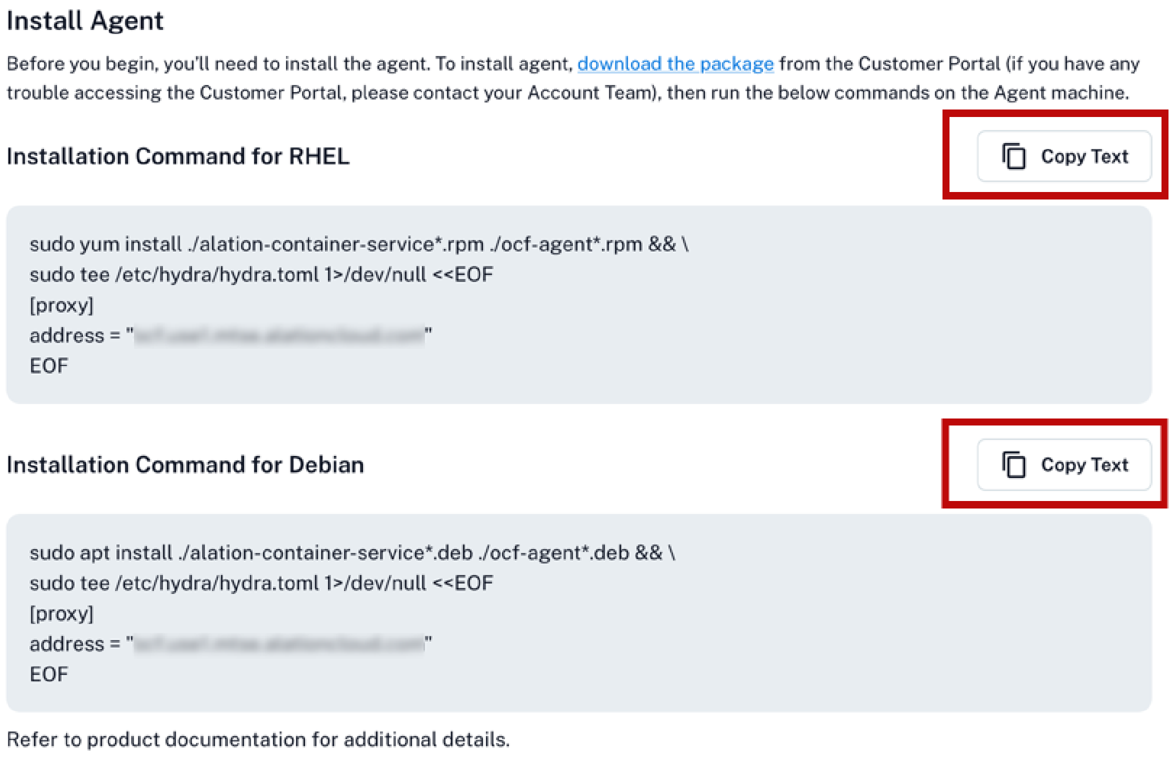
The Agent installation files are extracted into an **ocf-agent** directory.

5. Change into the ocf-agent directory.

```
cd ocf-agent
```

6. In Alation, copy the relevant installation command from the **Install Agent** screen.

New User Experience



Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

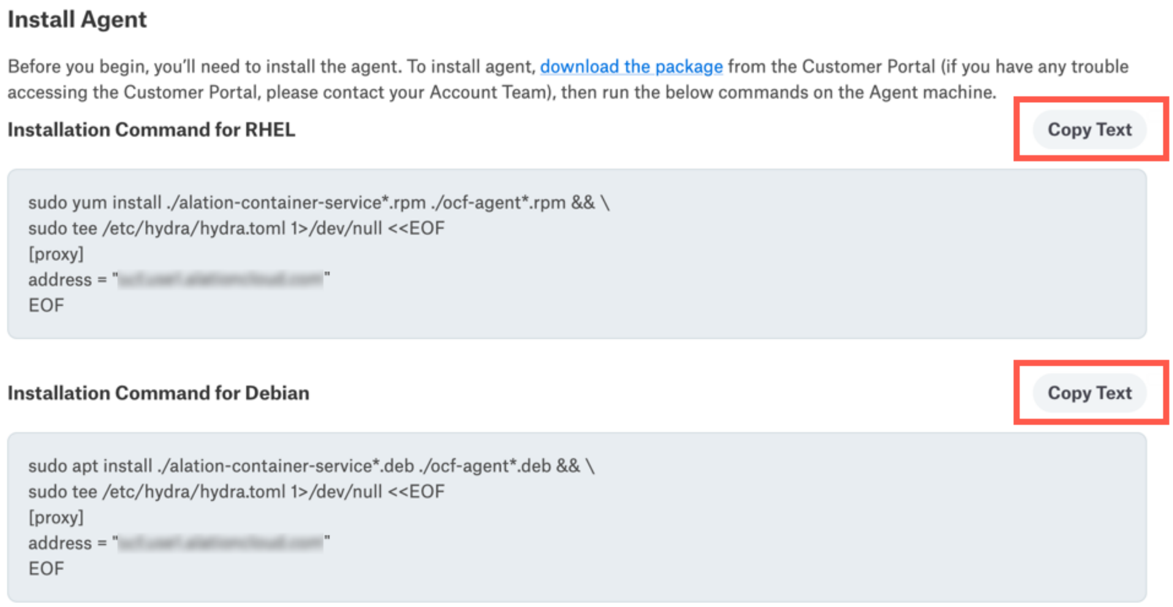
```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Installation Command for Debian

```
sudo apt install ./alation-container-service*.deb ./ocf-agent*.deb && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Refer to product documentation for additional details.

Classic User Experience



Install Agent

Before you begin, you'll need to install the agent. To install agent, download the package from the Customer Portal (if you have any trouble accessing the Customer Portal, please contact your Account Team), then run the below commands on the Agent machine.

Installation Command for RHEL

```
sudo yum install ./alation-container-service*.rpm ./ocf-agent*.rpm && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

Installation Command for Debian

```
sudo apt install ./alation-container-service*.deb ./ocf-agent*.deb && \
sudo tee /etc/hydra/hydra.toml 1>/dev/null <<EOF
[proxy]
address = "[redacted]"
EOF
```

7. In the terminal on the Agent's host machine, make sure you are in the **ocf-agent** directory, then paste and run the installation command. This will install and configure the Agent.
8. *(Optional)* If your network routes outgoing traffic through an HTTP CONNECT proxy, see the Advanced Configuration section below.
9. In Alation, click the **X** button to exit the **Add New Agent** dialog.

Note: Do not click the **Next** button. The remaining steps in the **Add New Agent** process are not needed in this scenario.

Advanced Configuration

If your network routes outgoing traffic through an HTTP CONNECT proxy, you need to:

- Add the Alation Cloud Service connectivity endpoint to your proxy server's allow list.
- Add the proxy's address to the Agent configuration file.

Proxy Allow List

You will need to add the Alation Cloud Service connectivity endpoint to your proxy server's allow list so the Agent can reach your Alation Cloud Service instance.

The Alation Cloud Service endpoint is shown on the `address` line of the Agent installation command. This is the same address that should be in your Agent configuration file at **/etc/hydra/hydra.toml**.

Add Proxy Address to Agent Config

This is done on the Agent's host machine. The steps depend on whether your proxy requires authentication.

- **No Authentication**

  For proxies that don't require authentication, edit **/etc/hydra/hydra.toml** to add the following line:

  ```
  web_proxy = "<proxy-address>:<proxy-port>"
  ```

- **Basic Authentication**

  Starting with Agent version 1.2.1.1168, you can route the Agent through proxies that require basic authentication. Edit **/etc/hydra/hydra.toml** to add the following line:

  ```
  web_proxy = "<username>:<password>@<proxy-address>:<proxy-port>"
  ```

  Replace the parts in angle brackets with the appropriate information for your proxy. Don't include the angle brackets. Do include the quotes. The proxy address can be a domain name or an IP address. If no port is provided, the Agent defaults to port 80.

  Here's an example with basic authentication:

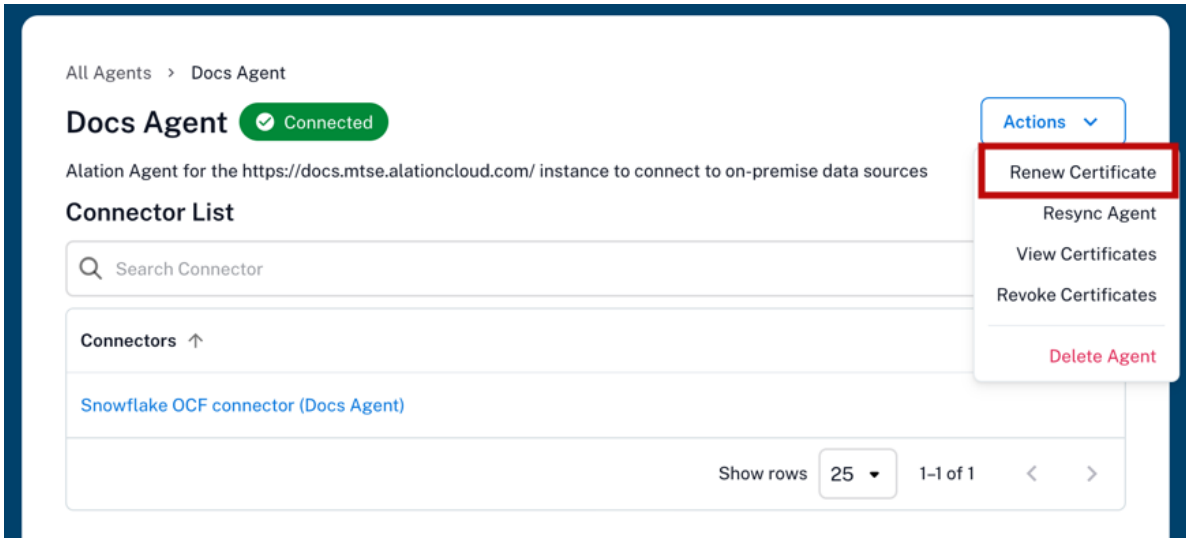
  ```
  web_proxy = "jane:securepassword@company.proxy.com:3128"
  ```

Step 4. Renew the Agent's Certificates

If you're reinstalling the Agent on the same machine as your old Agent, you may be able to reuse the old Agent's certificates. To check if your old Agent's certificates are still valid, see *View the Certificates' Expiration Date*. If they are not valid, or if you're installing the Agent on a new machine, use the steps below to renew the certificates.

1. On the **Agents Dashboard** in Alation, click the name of the Agent you are reconnecting to.
2. **New User Experience**

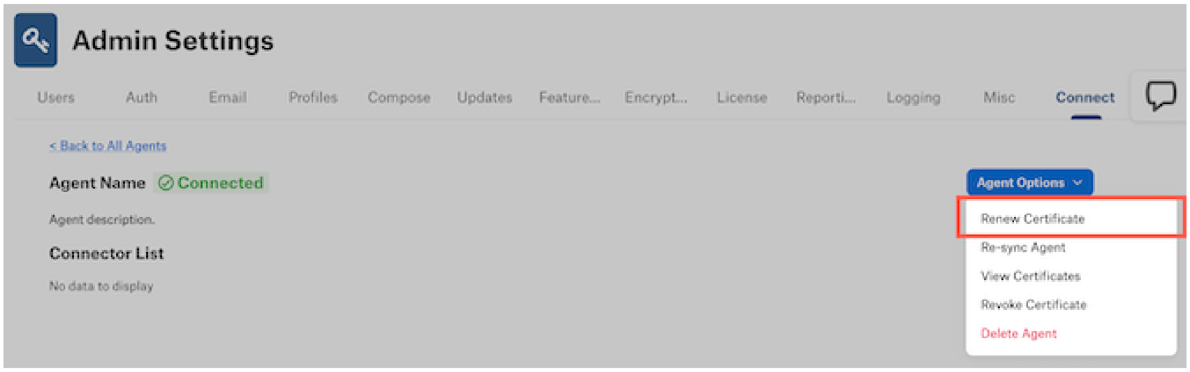
   Click the **Actions** button, then select **Renew Certificate**.



Alation Agent for the https://docs.mtse.alationcloud.com/ instance to connect to on-premise data sources

Classic User Experience

Click the **Agent Options** button, then select **Renew Certificate**.



3. On the **Generate Certificate Signing Request (CSR)** screen, copy the provided command and run it on the Agent's host machine.

```
sudo kratos certs gen
```

Since this Agent has already been connected to your Alation Cloud instance in the past, you will get a warning that a key has already been created.

```
Warning! A key for this agent appears to have already been generated
at "/etc/hydra/agent/security/proxy_key.pem". Generating a new key pair
will destroy the existing one.
Continue? [Y|n]
```

Enter **Y** to continue.

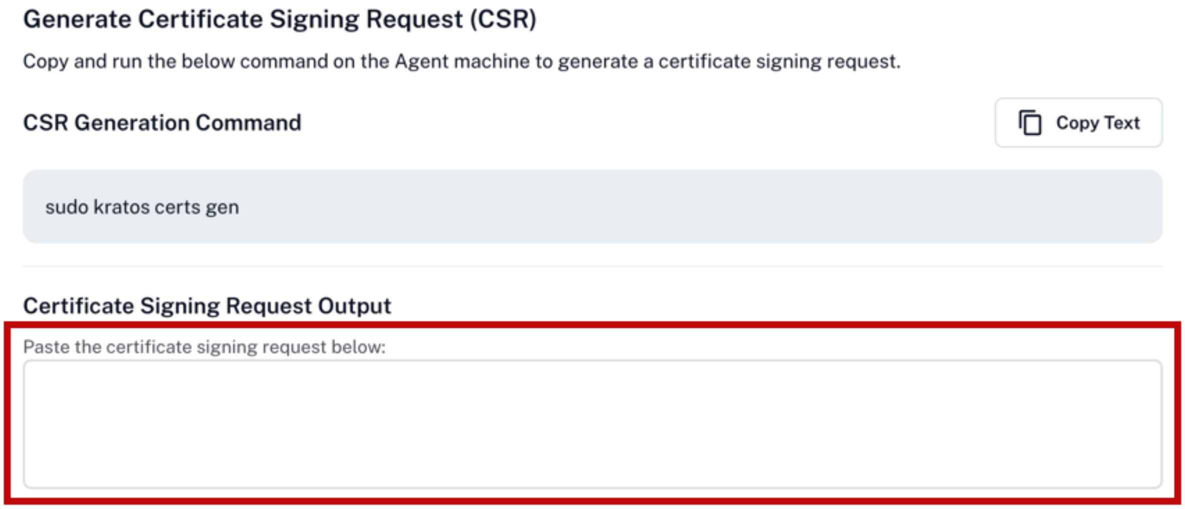
The command will generate a certificate signing request. Example output:

```
-----BEGIN CERTIFICATE REQUEST-----
<your certificate signing request>
-----END CERTIFICATE REQUEST-----
```

4. Copy the certificate signing request from the Agent machine, including the dashes.

5. In Alation, paste the certificate signing request into the provided box under **Certificate Signing Request Output**. Then click the **Next** button.

   New User Experience

   Generate Certificate Signing Request (CSR)

   Copy and run the below command on the Agent machine to generate a certificate signing request.

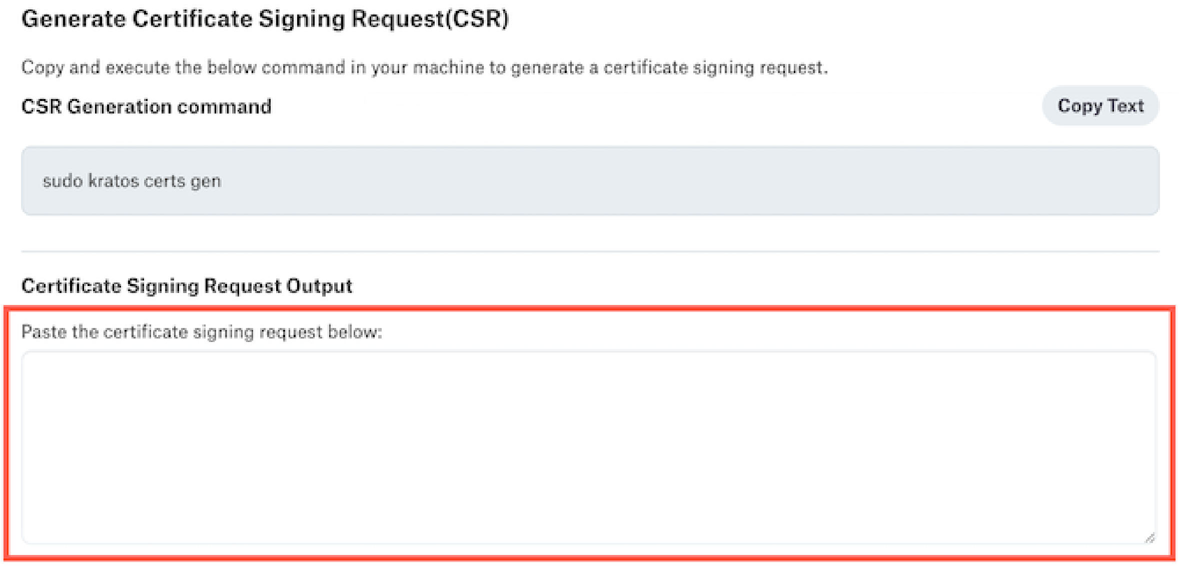
   CSR Generation Command

   ```
   sudo kratos certs gen
   ```

   Certificate Signing Request Output

   Paste the certificate signing request below:

   Classic User Experience

   Generate Certificate Signing Request(CSR)

   Copy and execute the below command in your machine to generate a certificate signing request.

   CSR Generation command

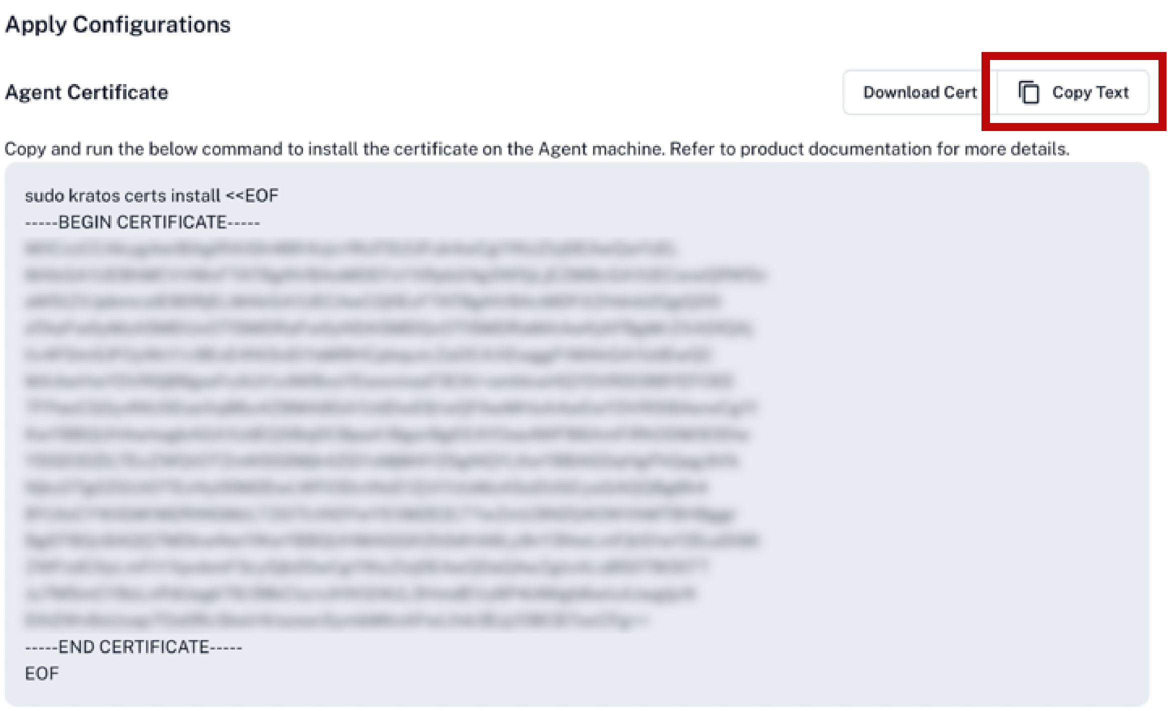
   ```
   sudo kratos certs gen
   ```

   Certificate Signing Request Output

   Paste the certificate signing request below:

6. Alation will generate two signed certificates—one for the Agent and one root certificate. Copy the provided certificate installation command.

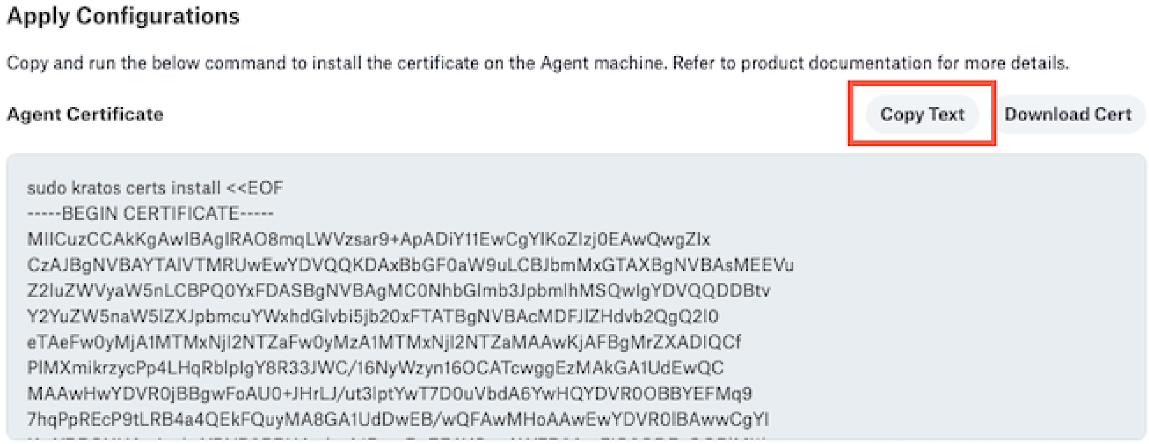
   New User Experience



Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
EOF
```

Classic User Experience



Copy and run the below command to install the certificate on the Agent machine. Refer to product documentation for more details.

```
sudo kratos certs install <<EOF
-----BEGIN CERTIFICATE-----
MIICuzCCAkKgAwIBAgIRAO8mqLWVzsar9+ApADiY11EwCgYIKoZIzj0EAwQwgZIx
CzAJBgNVBAYTAlVTMRUwEwYDVQQKDAxBbGF0aW9uLCBJbmMxGTAXBgNVBAsMEEVu
Z2luZWVyaW5nLCBPQ0YxFDASBgNVBAgMC0NhbGlmb3JpbmlhMSQwIgYDVQQDDBtv
Y2YuZW5naW5lZXJpbmcuYWxhdGlvbi5jb20xFTATBgNVBAcMDFJlZHdvb2QgQ2l0
eTAeFw0yMjA1MTMxNjI2NTZaFw0yMzA1MTMxNjI2NTZaMAAwKjAFBgMrZXADIQCf
PIMXmikrzycPp4LHqRblplgY8R33JWC/16NyWzyn16OCATcwggEzMAkGA1UdEwQC
MAAwHwYDVR0jBBgwFoAU0+JHrLJ/ut3lptYwT7D0uVbdA6YwHQYDVR0OBBYEFMq9
7hqPpREcP9tLRB4a4QEkFQuyMA8GA1UdDwEB/wQFAwMHoAAwEwYDVR0lBAwwCgYI
```

7. On the Agent’s host machine, paste the copied certificate command and run it. This installs the certificate.

8. Restart the Agent by copying the provided command and running it on the Agent’s host machine.

```
sudo systemctl restart hydra
```

9. When the Agent has finished restarting, click the **Finish** button in Alation. Check that your Agent has a status of **Connected** in the Agent Dashboard. If it doesn’t, check the *Troubleshooting* page.

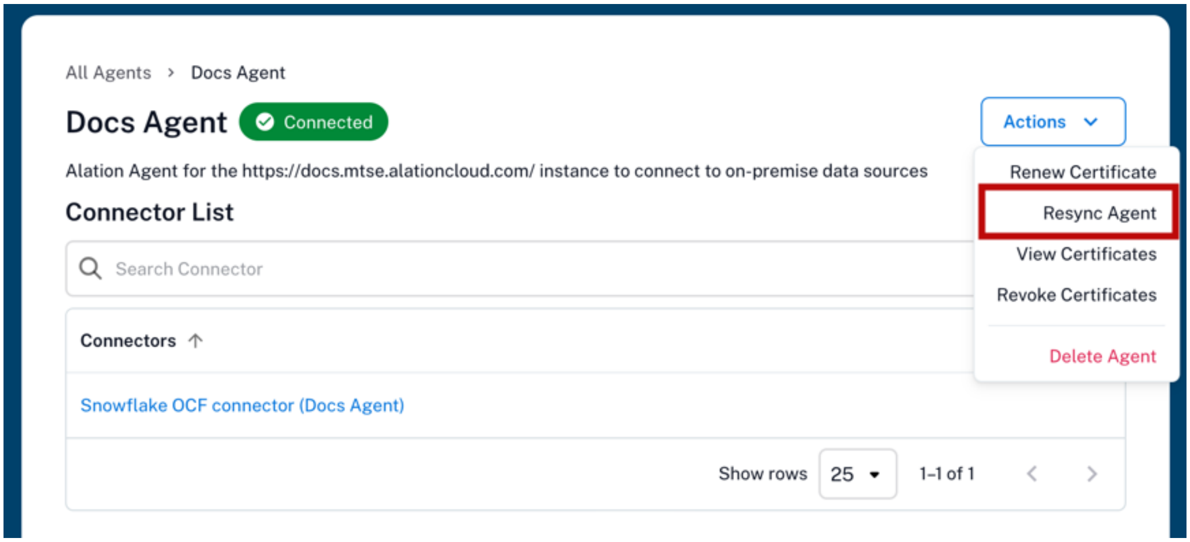
Warning: The certificates will automatically expire after one year.

Step 5. Resync the Agent

Your new Agent installation should now be connected to your Alation Cloud instance. Now you can resync the Agent, which will reinstall any connectors that you had previously installed on your Agent.

1. **New User Experience**

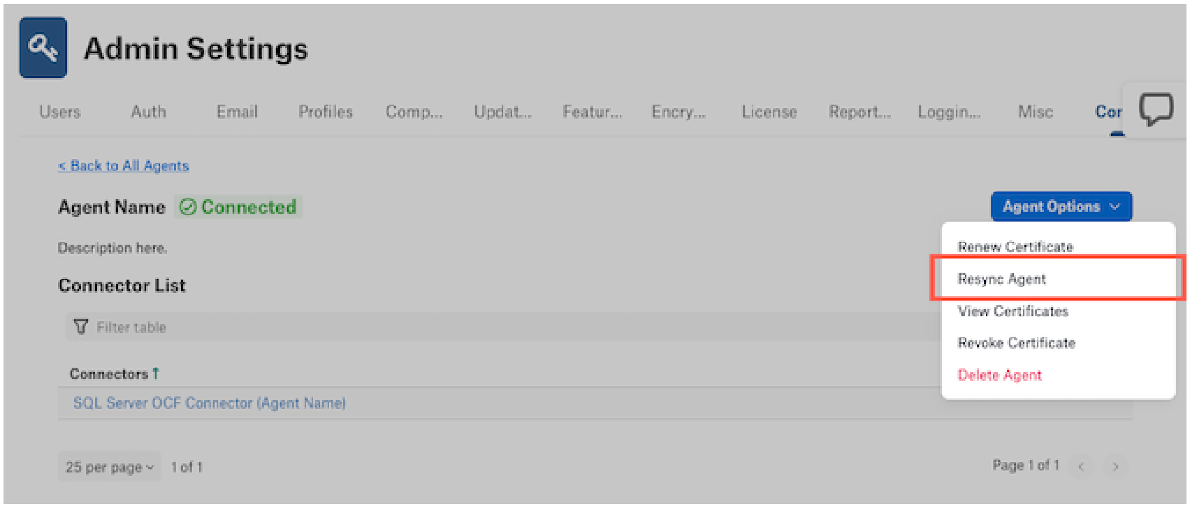
   Click the **Actions** button, then select **Resync Agent**.



Alation Agent for the https://docs.mtse.alationcloud.com/ instance to connect to on-premise data sources

   Classic User Experience

   Click the **Agent Options** button, then select **Resync Agent**.



Description here.

2. A confirmation message will appear. Click the **Confirm** button to continue resyncing.
3. The resync process may take some time. When the resync is complete, a success message will appear. Click the **Close** button.

Step 6. Verify the Data Source Connection

Now that the Agent has been resynced, you can verify that the Agent's data source is connected properly. To do this, you must be a Data Source Admin for the data source.

1. **New User Experience**

   Make sure the left navigation bar is expanded. Click **Data Sources**.

   Classic User Experience

   Go to **Apps** and select **Sources**.

2. Click the data source you want to verify.
3. **New User Experience**

   Click the three dot button on the upper right, then click **Settings**. Click **Continue to Classic Experience**.

   Classic User Experience

   Click on **More**, then **Settings**.

4. Click on the **General Settings** tab.
5. Under the **Network Connection** heading, click the **Test** button.

4.4.9 Start and Stop the Agent

Alation Cloud Service

On the Agent's host machine, you can start and stop the Agent if desired. Before starting or stopping the Agent, you may want to *check the Agent's status* first.

Stop the Agent

To stop a running Agent:

```
sudo hydra stop
```

Once the Agent has stopped, it will appear as disconnected on the **Agents Dashboard** in Alation. Running sudo docker ps on the Agent machine will show no active containers.

Start the Agent

To start a stopped Agent:

```
sudo hydra start
```

Restart the Agent

To restart the Agent (stop and then automatically restart again):

```
sudo hydra restart
```

4.4.10 Troubleshoot the Agent

Alation Cloud Service

This section will help you troubleshoot issues with the Agent. Issues may include:

- Agent is in a “Disconnected” status.
- Agent connectors are in an “Unknown” status.
- Error when installing new connectors.

If network interruptions ever break the connection between the Agent and your Alation Cloud instance, the Agent will attempt to reconnect. It keeps trying to connect using an exponential backoff algorithm. Once the Agent can connect to your Alation Cloud instance again, it will reauthenticate and reestablish a secure connection.

Any jobs, such as metadata extraction, that were underway will automatically restart as long as the connection is reestablished within 30 seconds. If it takes longer than that, you’ll have to restart the job manually.

Diagnose Agent Connectivity Problems

Applies to Agent versions 1.5.0.2541 and later

Alation Agent versions 1.5.0.2541 and later come packaged with a suite of diagnostics that you can use to troubleshoot connectivity issues when deploying the Agent. These checks include (but are not limited to):

- Operating system, memory, and CPU compatibility.
- Configuration of the Agent.
- Expired or revoked security certificates.
- Issues related to DNS resolution and establishment of a TCP connection to Alation Cloud Service.

To use the diagnostic tools, log into the Agent host machine. Some of the most useful commands are shown below.

To get help information about the diagnostics tool:

```
kratos diagnostics help
```

To save the logs for all Agent *components*, including connectors, to the /**tmp** directory:

```
kratos diagnostics logs -o /tmp
```

To get a list of available diagnostics:

```
kratos diagnostics list
```

To run all diagnostics and save the results to a file:

```
kratos diagnostics run >> agent_diagnostics.yaml
```

You can send the resulting file, which includes the output logs of the diagnostics, to Alation Support to enable faster diagnosis of Agent connectivity problems.

Check the System Requirements

Verify that the Agent's host machine meets the *Agent System Requirements*.

Check the Agent Version

Ensure that you have installed the latest version of the Agent.

1. On the Agent host machine, check the installed Agent's version by running:

   ```
   hydra version
   ```

   The version number will be in the first line of the output.

2. Go to the Alation Customer Portal. If prompted, log in.

3. On the Alation Customer Portal, check the latest version number under the **Version** column. If it's newer than the Agent you have installed, *upgrade the Agent*.

Check the Agent's Status

As a troubleshooting step, or when starting and stopping the Agent, you may want to check the Agent's status.

Agent Status in Alation

New User Experience

In Alation, you can check the Agent's connection status by visiting **Admin Settings** > **Agents**.

Classic User Experience

In Alation, you can check the Agent's connection status by visiting **Admin Settings > Manage Connectors > Agents Dashboard**.

The Agent's **Status** tells you if your Alation Cloud instance can reach the Agent.

Agent Status on the Agent's Machine

You can check the status of the Agent's individual components on the Agent's host machine. To check the status, run the following command:

```
sudo docker ps
```

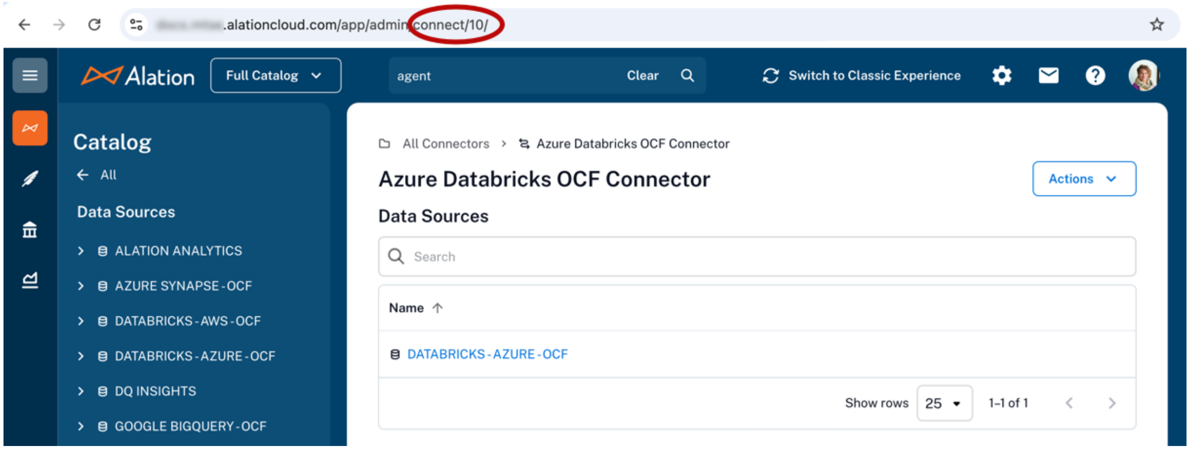
This command will output a list of running Docker containers. A normally functioning Agent will show several containers:

- **agent:** This is the component that manages the connectors that are installed on the Agent.

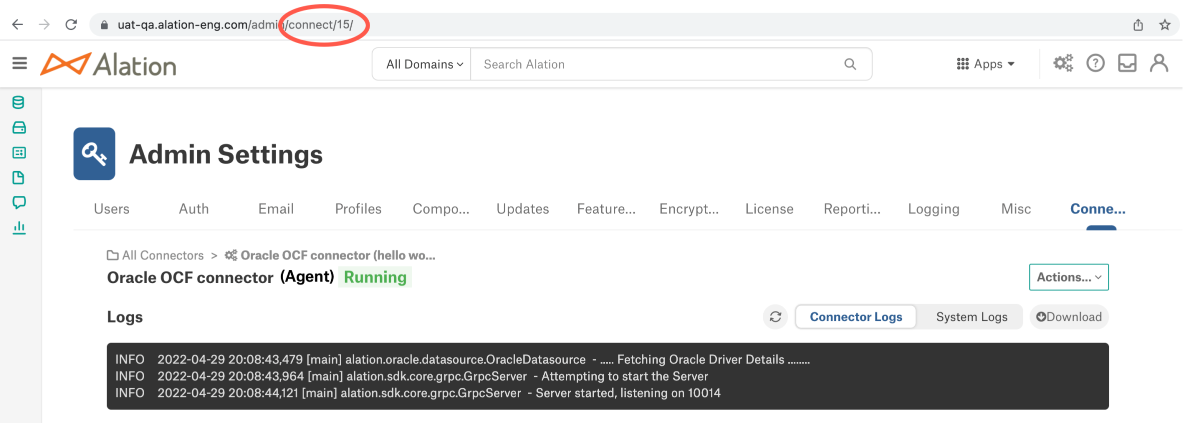
- **proxy:** This is the component of the Agent that communicates with Alation Cloud Service.
- **auth:** This is the Authentication Service add-on, if installed.
- **connector_[n]:** Each connector will be listed with **n** representing the connector's ID.

  You can correlate the ID with the connectors on the **Connectors Dashboard** in Alation by clicking on a connector and viewing its URL.

  New User Experience



  Classic User Experience



```
INFO   2022-04-29 20:08:43,479 [main] alation.oracle.datasource.OracleDatasource  - ..... Fetching Oracle Driver Details ........
INFO   2022-04-29 20:08:43,964 [main] alation.sdk.core.grpc.GrpcServer  - Attempting to start the Server
INFO   2022-04-29 20:08:44,121 [main] alation.sdk.core.grpc.GrpcServer  - Server started, listening on 10014
```

If any components are missing from the list, that means they are not running. You can try to start the components back up by running `sudo hydra restart` on the Agent machine. Then run `sudo docker ps` again to check the status.

Check the Certificates

If the Agent shows as disconnected, it may be that the Agent's certificates have expired or been revoked. The certificates expire automatically after one year.

To check if the Agent has valid certificates, see *View the Certificates' Expiration Date*. If the Agent does not have valid certificates, see *Renew the Certificates* to reestablish the connection. Do not add a new Agent, as doing so will not solve problems with certificates and may cause additional problems.

Update the Agent's Address Configuration

If the Agent is in a disconnected status, you may need to update the Agent's address configuration. For instructions, see *Update the Agent's Address Configuration*

Check Agent Error Messages

To view Agent error messages, run the following command on the Agent's host machine:

```
sudo systemctl status hydra.service
```

Check Logs

Each *component* of the Agent writes its own logs on the Agent host machine. Each connector that's installed on the Agent also has its own logs. On the Agent machine, you can get an archive of all logs or check the logs for each component and connector separately. Connector logs are also available directly in Alation.

All Logs

You can get an archive of all Agent component logs, including connector logs, using the Agent diagnostics tool on the Agent machine.

To save all Agent logs to the current working directory:

```
kratos diagnostics logs
```

To save all Agent logs to a specified directory:

```
kratos diagnostics logs -o /tmp
```

Agent Component Logs

To check the Agent's logs, you'll need to know the name of the Docker container for the component you're checking. To get the names of the containers, run the following command on the Agent's host machine:

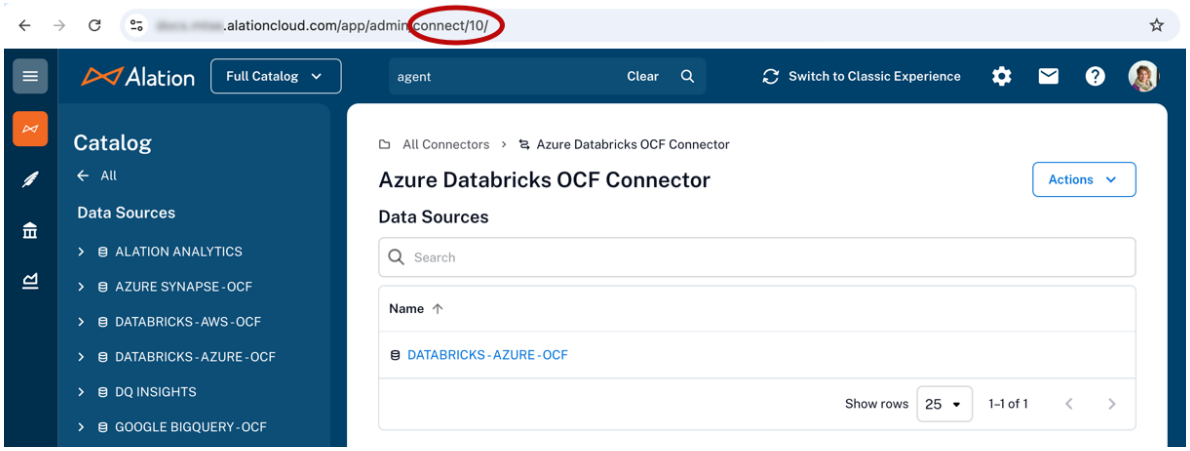
```
sudo docker ps
```

In the output, the **NAMES** column shows a list of the Agent's components.

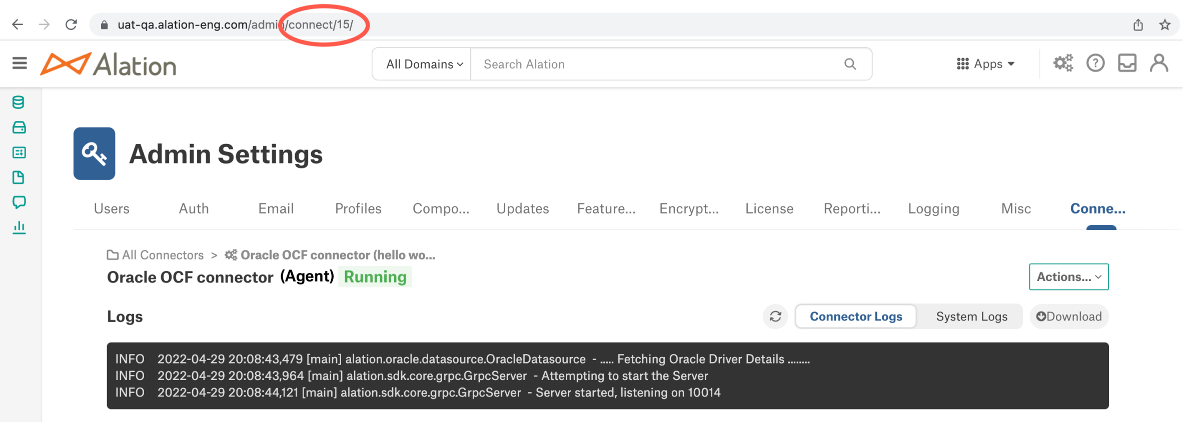
- **agent:** This is the component that manages the connectors that are installed on the Agent.
- **proxy:** This is the component of the Agent that communicates with Alation Cloud Service.
- **auth:** This is the Authentication Service add-on, if installed.
- **connector_[n]:** Each connector will be listed with **n** representing the connector's ID.

  You can correlate the ID with the connectors on the **Connectors Dashboard** in Alation by clicking on a connector and viewing its URL.

  New User Experience



Classic User Experience



```
INFO   2022-04-29 20:08:43,479 [main] alation.oracle.datasource.OracleDatasource  - ..... Fetching Oracle Driver Details ........
INFO   2022-04-29 20:08:43,964 [main] alation.sdk.core.grpc.GrpcServer  - Attempting to start the Server
INFO   2022-04-29 20:08:44,121 [main] alation.sdk.core.grpc.GrpcServer  - Server started, listening on 10014
```

Access the logs using the `docker logs` command followed by the name of the container. For example:

```
# tail logs for Alation Connector Manager component
docker logs -f agent
# tail logs for proxy component
docker logs -f proxy
# tail logs for the Authentication Service add-on, if installed
docker logs -f auth
# save logs to a file
docker logs agent >& agent.logs 2>&1
docker logs proxy >& agent.logs 2>&1
```

Connector Logs

Each OCF connector has logs that record information about actions such as metadata extraction and query log ingestion. Logs for OCF connectors installed on the Agent are available from the **Connectors Dashboard**. See Connector Logs for more information.

To view OCF connector logs on the Agent's host machine:

1. Get the ID of the connector by running `kratos list` and looking for the "id" field. Or run `sudo docker ps` and look for the number following the underscore in the container name.
2. Use the commands below to work with the connector logs as desired:

```
# Tail logs
kratos tail <ID>

# Get full logs
kratos logs <ID>

# Get logs from a specific date
kratos logs --since 2024-08-15 <ID>

# Redirect logs to a file
kratos logs <ID> > connector_3.log 2>&1
```

4.4.11 Alation Agent Version History

Alation Cloud Service

In the table below, find the version of Alation you're currently using. To get the latest Alation Agent features and fixes, we recommend *upgrading* to the latest version of the Alation Agent that's compatible with your version of Alation Cloud Service.

Alation provides downloads for the latest two versions of the Alation Agent on the Customer Portal. Older versions of the Agent will become unavailable as newer versions are released.

Alation Agent Version	Compatible Versions of Alation Cloud Service
1.7.3.4537	2024.1.4, 2024.1.5, 2024.3
1.7.3.4452	2024.1.3, 2024.1.4 , 2024.3
1.7.2.4360	2024.1.3, 2024.1.4
1.7.0.4045	2024.1.1, 2024.1.2, 2024.1.3, 2024.1.4
1.6.1.3465	2023.3.4, 2023.3.5, 2024.1, 2024.1.1
1.6.1.3288	2023.3.4, 2023.3.5
1.5.1.2863	2023.1.7, 2023.3.1, 2023.3.2, 2023.3.3
1.5.0.2541	2023.1.7, 2023.3
1.3.0.1536	2022.4, 2023.1, 2023.1.1 to 2023.1.7
1.2.1.1168	2022.4, 2023.1
1.2.1.1120	2022.4
1.2.1.868	2022.3, 2022.4, 2023.1
1.2.0.815	2022.2, 2022.3